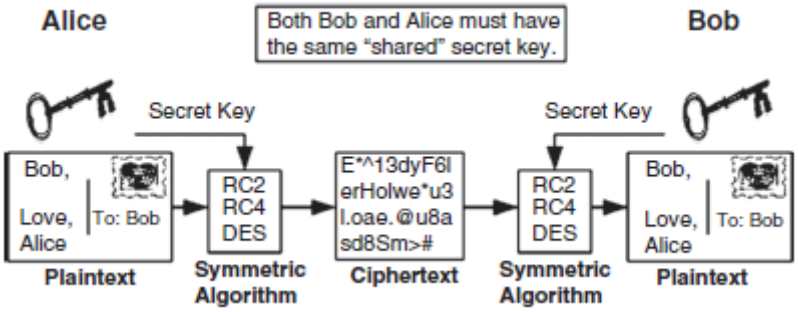
PKI I ORGANY CERTYFIKACYJNE

WPROWADZENIE

W latach 90. szyfrowanie w Internecie polegało głównie na wymianie bezpiecznych wiadomości e-mail przez osoby z Pretty Good Privacy (PGP), a później przez Gnu Privacy Guard (GnuPG, pierwotnie w skrócie GPG), z których każda utrzymywała prywatną sieć zaufania. szyfrowanie obejmuje znacznie szerszy zakres elementów, w tym sprawdzanie, wydawanie, unieważnianie, identyfikację, federację, mostkowanie, szyfrowanie, podpisywanie cyfrowe i niezliczone procesy pomocnicze. W rzeczywistości to, czego doświadcza użytkownik, jest tylko wierzchołkiem wymaganej konstrukcji wsporczej. Właściwe zarządzanie informacjami związanymi z infrastrukturą szyfrowania (lub kryptosystemem) dotyczy zaufania, tego, co jest wymagane do ustanowienia tego zaufania i ile przyznać. W tamtych czasach szyfrowanie było najczęściej wykorzystywane poza obrębem sieci, gdzie niezabezpieczone dane wysyłane i odbierane przez organizację za pośrednictwem sieci publicznych były postrzegane jako najbardziej narażone na ataki ujawnienia, modyfikacji, wstawiania, usuwania i powtarzania. Aby chronić dane przesyłane przez niezaufane sieci, jedyną praktyczną i opłacalną technologią jest kryptografia. Kryptografia jest sercem zarówno wirtualnych sieci prywatnych (VPN), jak i infrastruktury klucza publicznego.

Kryptografia klucza symetrycznego.

Kryptografia symetryczna (znana również jako pojedynczy klucz lub klucz tajny) używa tego samego klucza do szyfrowania zwykłego tekstu na tekst zaszyfrowany i odszyfrowywania zaszyfrowanego tekstu z powrotem do zwykłego tekstu. Proces ten ilustruje Rysunek.



Chociaż kryptografia symetryczna (np. Advanced Encryption Standard [AES], Data Encryption Standard [DES], Rivest Cipher 4 [RC4]) ma szczególne zalety, ponieważ ma gęstą przestrzeń kluczy (dowolna liczba całkowita) i jest bardzo szybka obliczeniowo, ma fundamentalna słabość: klucz musi mieć zarówno pomysłodawca, jak i każdy odbiorca. Udostępnianie kluczy wiąże się z dwoma problemami związanymi z zarządzaniem:

1. Należy przeprowadzić wymianę klucza: w jakiś sposób każdy użytkownik musi mieć ten sam klucz. Ta wymiana jest zazwyczaj realizowana poza pasmem.

2. Poufność, kontrola lub uwierzytelnianie są słabe: każdy, kto ma klucz symetryczny, mógł zaszyfrować tekst jawny lub odszyfrować tekst zaszyfrowany.

Kryptosystem klucza publicznego

W przeciwieństwie do kryptosystemów z kluczem tajnym, kryptosystemy z kluczem publicznym (PKC) używają par powiązanych ze sobą kluczy, które są generowane razem. Przyjmuje się, że generowanie

jednego klucza z drugiego jest niewykonalne. Zaszyfrowany tekst utworzony przez jeden klucz można odszyfrować tylko za pomocą drugiego członka tej samej pary kluczy. Jeden z tych kluczy jest utrzymywany w tajemnicy (klucz prywatny), a drugi jest publikowany do użytku wszystkich (klucz publiczny). Nie ma znaczenia, który jest oznaczony jako który, ale raz wyznaczony klucz nie może zostać zmieniony. W praktyce szyfrowanie jednym kluczem jest często szybsze niż drugim. Ten jest zwykle wybierany jako klucz publiczny. W najprostszej formie, aby ukryć przesyłaną wiadomość, aby tylko żądany odbiorca mógł ją przeczytać, jawny tekst jest szyfrowany przy użyciu klucza publicznego odbiorcy. Tylko tajny klucz odbiorcy może odszyfrować przesłany zaszyfrowany tekst. Podobnie, aby zweryfikować integralność i autentyczność wiadomości, możliwe jest zaszyfrowanie informacji za pomocą klucza prywatnego nadawcy. Dzięki temu każdy, kto ma dostęp do klucza publicznego tego nadawcy, może zweryfikować wiadomość przez pomyślne odszyfrowanie zaszyfrowanego tekstu.

Zalety kryptosystemu klucza publicznego w porównaniu z kryptosystemem kluczem tajnego

W celu zabezpieczenia transmisji danych, systemy kryptograficzne z kluczem publicznym są preferowane w stosunku do systemów kryptograficznych z kluczem tajnym z następujących powodów:

* Kryptosystemy klucza publicznego wymagają mniejszej liczby kluczy do zarządzania: każda strona (n) ma parę kluczy, więc całkowita liczba kluczy wynosi 2n, zamiast być proporcjonalna do n2 jak w przypadku kryptosystemów z kluczem tajnym.

* Ponieważ klucze prywatne nie muszą być dystrybuowane ani zarządzane w inny sposób, kryptosystemy klucza publicznego wymagają jedynie wykazania integralności i autentyczności samych kluczy publicznych. Użytkownicy (strony ufające) muszą mieć pewność, że ich klucze publiczne naprawdę należą do wydawców. Wymaga to podpisania przez zaufaną stronę trzecią lub wzajemnie zaufane źródło.

* Ponieważ żadne tajne klucze nie są przesyłane przez żadną sieć, pakiety PKC nie są podatne na złamanie, nawet jeśli trzeba zmienić klucze publiczne. Kody PKC mogą służyć do szyfrowania kluczy tymczasowych (kluczy sesji), których można użyć jednorazowo do kryptografii klucza tajnego w celu uniknięcia większego obciążenia obliczeniowego PKC.

* Aby zaszyfrować wiadomość, aby wielu użytkowników PKC mogło bezpiecznie odbierać i odszyfrowywać zaszyfrowany tekst, oprogramowanie PKC może utworzyć klucz sesji. Ten tajny klucz jest następnie szyfrowany oddzielnie kluczem publicznym każdego odbiorcy i wysyłany wraz z zaszyfrowanym tekstem do wszystkich odbiorców bez naruszania poufności. Każdy odbiorca może następnie wyodrębnić klucz użyty do zaszyfrowania pliku.

Podpisy cyfrowe oparte na PKC mogą również stanowić podstawę do niezaprzeczalności w przypadku sporu. Tylko posiadacz klucza prywatnego mógł wysłać wiadomość odszyfrowaną przez jego klucz publiczny. W przeciwieństwie do tego, ze względu na użycie współdzielonych kluczy tajnych, same kryptosystemy symetrycznego klucza tajnego nie mogą rozsądnie wspierać niezaprzeczalności.

Połączenie Dwóch

W tym momencie najłatwiej będzie rozważyć elementy różnych typów kryptografii. Różnica jest podobna do tej między elektroniczną wymianą danych a e-commerce. Szyfrowanie symetryczne jest dobre w przypadku bardzo niewielu wymian z zaufanymi osobami; szyfrowanie asymetryczne jest dobre dla wielu, wielu małych wymian z osobami lub urządzeniami, których być może nigdy nie spotkałeś. Obecnie najczęstszym zastosowaniem jest łączenie obu typów: aby dokument mógł zostać bezpiecznie wysłany pocztą elektroniczną, wybierany jest algorytm symetryczny i generowany losowo klucz. Dokument jest szyfrowany przy użyciu algorytmu i klucza symetrycznego. Klucz symetryczny jest

następnie szyfrowany asymetrycznym kluczem publicznym każdego odbiorcy, a następnie dodawany jako nagłówek do dokumentu. W przypadku podpisów cyfrowych stosuje się podobny mechanizm, z tym że algorytm haszujący (np. Secure Hash Algorithm [SHA]) jest używany do tworzenia wartości skrótu dokumentu, a następnie hasz jest szyfrowany (podpisywany) kluczem prywatnym inicjatorem i towarzyszy dokumentowi. Klucz publiczny nadawcy może być użyty do odszyfrowania (weryfikacji) skrótu, a skrót służy do weryfikacji integralności dokumentu.

POTRZEBA INFRASTRUKTURY KLUCZU PUBLICZNEGO

PKC zależy od integralności każdego klucza publicznego i powiązania tego klucza publicznego z konkretnym podmiotem, takim jak osoba, instytucja lub element sieci. Bez mechanizmów zapewniających integralność i autentyczność strona ufająca jest narażona na ataki maskarady poprzez podstawienie klucza publicznego. Aby to zilustrować, załóżmy, że firma ABC chce wysłać do XYZ Corp. poufną wiadomość, której nikt inny nie może przeczytać. ABC mogłoby użyć klucza publicznego XYZ do zaszyfrowania wiadomości, chociaż, ze względu na wydajność, ABC prawdopodobnie użyłoby algorytmu symetrycznego do zaszyfrowania wiadomości i algorytmu klucza publicznego do zaszyfrowania klucza symetrycznego. Jednakże, jeśli ABC można nakłonić do użycia klucza publicznego napastnika tak, jakby to był klucz publiczny XYZ, to atakujący będzie mógł odszyfrować wiadomość. Ta technika jest znana jako fałszowanie klucza publicznego. Takie fałszowanie klucza publicznego przez atakującego uniemożliwiłoby jednak XYZ odczytanie wiadomości z ABC, jak pierwotnie zamierzano. Dlatego taki atak prawdopodobnie kontynuowałby atak, który ponownie zaszyfrowałby wiadomość ABC przy użyciu prawdziwego klucza publicznego XYZ i wysłał go do XYZ. Takie przechwytywanie i ponowne szyfrowanie jest przykładem ataku typu man-in-the-middle. Jeśli jednak nadawca również podpisał oryginalną wiadomość, jest to coś, czego atakujący nie mógł powielić, więc wiadomości nie można zmienić, a jedynie przechwycić. Innym przykładem naruszenia połączenia między kluczem publicznym a jego właścicielem jest weryfikacja podpisu cyfrowego. Załóżmy, że ABC chce zweryfikować podpis XYZ. Jeśli atakujący mógłby nakłonić ABC do użycia klucza publicznego atakującego tak, jakby był to klucz publiczny XYZ, wówczas osoba atakująca byłaby w stanie podpisywać wiadomości podszywające się pod XYZ przy użyciu klucza prywatnego atakującego. ABC nieświadomie użyje zastąpionego klucza publicznego i zostanie podszyte, myśląc, że wiadomość faktycznie została podpisana przez XYZ. Ten sam problem występuje w rdzeniu dzisiejszego handlu internetowego — Secure Sockets Layer v2 (SSLv2). SSLv3 i Transport Layer Security (TLS) mogą temu zapobiec, ale wtedy każdy uczestnik musi mieć certyfikat zaufany przez drugą stronę. W tym miejscu pojawia się koncepcja łańcucha zaufania. Jeśli zaufana strona trzecia podpisała klucz publiczny XYZ, atakujący również musiałby mieć klucz podpisany przez ten sam organ. W przeciwnym razie pojawiłoby się ostrzeżenie, że klucz nie został rozpoznany. Poważnym problemem jest sama liczba urzędów certyfikacji (ponad 100) wbudowanych w większość przeglądarek z różnych krajów. Przeglądarka domyślnie ufa wszystkim certyfikatom wystawionym przez którykolwiek z nich i niekoniecznie wszystkie są godne zaufania. Podsumowując, zarówno w przypadku usług podpisu cyfrowego, jak i szyfrowania, strona ufająca musi używać klucza publicznego właściwej strony w celu zachowania bezpieczeństwa. Istnieją różne ręczne, elektroniczne i hybrydowe mechanizmy dystrybucji kluczy publicznych w sposób zaufany, dzięki czemu strona ufająca może mieć pewność, że posiada prawidłowe klucze publiczne subskrybentów. Te mechanizmy dystrybucji i wiązania kluczy publicznych są znane jako infrastruktura klucza publicznego (PKI). Piękno podpisanego klucza publicznego polega na tym, że zaufanie jest nieodłącznie związane z podpisem, pod warunkiem, że osoba podpisująca jest zaufana. W przeciwieństwie do sieci zaufania, takiej jak ta używana przez oryginalny PGP, która wymaga, aby wszystkie klucze były akceptowane indywidualnie przez każdego użytkownika, w łańcuchu zaufania pojedynczy podpisujący (główny urząd certyfikacji) może zapewnić zaufanie milionom certyfikatów. Zaufanie nie musi być absolutne; może to być kontekstowe. Na przykład

certyfikat podpisany przez pracodawcę można ufać w odniesieniu do elementów związanych z zatrudnieniem, ale nie w przypadku kart kredytowych.

CERTYFIKAT KLUCZA PUBLICZNEGO

Najbardziej skalowalna technika wykorzystuje certyfikat klucza publicznego wystawiony przez zaufaną stronę zwaną urzędem certyfikacji (CA). CA wydaje certyfikaty klucza publicznego różnym subskrybentom, łącząc informacje o subskrybentach i podpisując je za pomocą klucza prywatnego CA. Ogólnie przyjętym standardem dla certyfikatów klucza publicznego jest X.509 w wersji 3,2 zgodnie z definicją w RFC 5280 i późniejszym tekście.

Uwaga: struktury hierarchiczne mogą wykorzystywać jeden lub więcej głównych urzędów certyfikacji, a każdy główny urząd certyfikacji może mieć wiele pośrednich urzędów certyfikacji, które wystawiają certyfikaty użytkownika końcowego i serwera

Certyfikaty X.509 są wyrażone w notacji Abstract Syntax Notation 1 (ASN.1), która jest złożoną notacją binarną. Aby mogły zostać przekazane przez e-mail, certyfikaty są zwykle zakodowane w MIME (czyli Base 64), wyrażając składnię binarną w znakach ASCII. Zaletą korzystania z urzędu certyfikacji i łańcucha zaufania jest to, że ufając rootowi, użytkownik automatycznie ufa wszystkim kluczom, które wydał, niezależnie od tego, czy użytkownik kiedykolwiek je widział. Każdy certyfikat CA może zawierać następujące kluczowe informacje:

* Numer wersji standardu certyfikatu

* Numer seryjny certyfikatu (unikalny dla każdego certyfikatu wydanego przez CA)

* Algorytm i powiązane parametry używane przez CA do podpisywania certyfikatu

* Nazwa urzędu certyfikacji

* Okres ważności certyfikatu

* Nazwa subskrybenta

* Klucz publiczny subskrybenta, algorytm klucza publicznego i powiązane parametry

* Unikalny identyfikator urzędu certyfikacji (opcjonalnie)

* Unikalny identyfikator subskrybenta (opcjonalnie)

* Rozszerzenia (opcjonalnie)

* Cyfrowy podpis CA

Strony ufające wymagają klucza publicznego CA, aby móc zweryfikować podpisy cyfrowe certyfikatów wydanych przez CA. Strona ufająca musi zaufać kluczowi publicznemu CA, najprawdopodobniej uzyskanemu podczas procesu rejestracji. Po zweryfikowaniu podpisów strony ufające mogą używać nazwy subskrybenta i klucza publicznego subskrybenta w certyfikacie z takim samym zaufaniem co do dokładności informacji, jak zaufanie urzędu certyfikacji. W niektórych sytuacjach może wystąpić konieczność odwołania przez urząd certyfikacji powiązania między subskrybentem a kluczem publicznym tego subskrybenta. Na przykład klucz prywatny subskrybenta może zostać skompromitowany (tj. mogą istnieć powody, by sądzić, że klucz tajny wpadł w ręce kogoś innego). Ponieważ certyfikat klucza publicznego jest obiektem elektronicznym i może znajdować się w kilku miejscach jednocześnie, nie jest ani praktyczne, ani możliwe, aby przywołać, usunąć lub wymazać wszystkie kopie certyfikatu subskrybenta w środowisku rozproszonym. Tak więc, aby unieważnić

certyfikat klucza publicznego przez zerwanie powiązania między subskrybentem i kluczem publicznym subskrybenta, CA tworzy listę nieważnych certyfikatów. Ta lista nazywana jest listą odwołania certyfikatów (CRL). Strony ufające muszą sprawdzić, czy certyfikat nie znajduje się na liście CRL przed użyciem klucza publicznego w certyfikacie. Jeśli certyfikat znajduje się na liście CRL, strona ufająca nie może z niego korzystać. CA podpisuje listę CRL, aby umożliwić stronom ufającym zweryfikowanie integralności i autentyczności listy CRL. Kluczowe informacje w liście CRL X.509 w wersji 2 to:

* Numer wersji standardu CRL

* Algorytm i powiązane parametry używane przez CA do podpisywania certyfikatu

* Nazwa urzędu certyfikacji

* Ten czas wystawienia listy CRL

* Czas następnego wystawienia listy CRL (opcjonalnie)

* Lista unieważnionych certyfikatów (wymienianie tych pozycji dla każdego certyfikatu):

* Numer seryjny certyfikatu

* Czas powiadomienia CA o unieważnieniu

* Rozszerzenia związane z unieważnionym certyfikatem (opcjonalnie)

* Rozszerzenia związane z listą CRL (opcjonalnie)

* Podpis cyfrowy A

Ważne jest, aby certyfikat zawierał tylko te elementy, które są konkretnie wymagane do działania i aby były one właściwie używane, w przeciwnym razie może dojść do pomyłki i niewłaściwego/nieoczekiwanego użycia. Prawdopodobnie najczęściej używanym elementem jest rozszerzenie Key Usage. (Jest używany tak źle, że często drugie rozszerzenie, Rozszerzone użycie klucza, jest używane do wyjaśnienia pierwszego). Najczęstszym błędem jest ustawienie bitu niezaprzeczalności na kluczu przeznaczonym wyłącznie do identyfikacji. Niezaprzeczalność powinna być zapewniona tylko na kluczu przeznaczonym jako podpis prawny, a nie tylko dla tożsamości. Niebezpiecznym rozszerzeniem (i takim, które tak naprawdę nie należy do certyfikatu użytkownika) jest rozszerzenie SMIME Capabilities. Ma to znaczenie tylko w kontekście konkretnych klientów poczty e-mail, ale może utrudnić korzystanie z szyfrowania. Chociaż mógł mieć pewne zastosowanie we wczesnych aplikacjach pocztowych, obecnie ustanawia tylko maksymalną dozwoloną siłę szyfrowania symetrycznego, która może być mniejsza niż oczekiwana. Jeśli to rozszerzenie nie jest obecne, RFC 5280 wymaga domyślnego potrójnego DES. W przypadku certyfikatów mniej znaczy więcej. Minimalna liczba pól i rozszerzeń wymaganych dla asercji, jakie ma tworzyć certyfikat, jest najlepsza. Systemy PKI w przeszłości zawiodły, gdy dodano zbyt wiele, czasami sprzecznych z misją rozszerzeń. Należy zwrócić szczególną uwagę, aby wybrany dostawca serwera CA nie dodał niczego, co nie jest określone przez szablon certyfikatu w Polityce Certyfikacji.

INFRASTRUKTURA KLUCZU PUBLICZNEGO PRZEDSIĘBIORSTWA

Użycie certyfikatu jest stosunkowo proste, ale ustanowienie zaufania, że certyfikat jest ważny i odpowiedni do użycia, wymaga złożonego zestawu elementów back-office, zilustrowanych na Dowodzie 37.4. Każda grupa użytkowników objęta CA nazywana jest domeną. Subskrybenci w domenie otrzymują certyfikaty klucza publicznego z odpowiedniego urzędu certyfikacji. CA odpowiada za

generowanie certyfikatów subskrybenta oraz generowanie list CRL. Urząd certyfikacji publikuje te podpisane obiekty w repozytorium, gdzie strony ufające mogą je uzyskać. CA archiwizuje również certyfikaty i listy CRL na wypadek, gdyby były one potrzebne w przyszłości do rozstrzygania sporów między subskrybentami a stronami ufnymi. Urząd rejestracji (RA) jest zaufanym przedstawicielem urzędu certyfikacji i odpowiada za uwierzytelnianie tożsamości subskrybenta. RA zazwyczaj wykonuje te funkcje:

* Uwierzytelnia (dowodzi) deklarowaną tożsamość subskrybenta. Na przykład RA może wymagać od subskrybenta dostarczenia ważnego dokumentu tożsamości ze zdjęciem, takiego jak prawo jazdy lub paszport, aby zapewnić minimalną pewność. Zarówno uwierzytelnienie I-9, zgodnie z wymogami Ustawy o reformie i kontroli imigracyjnej (IRCA), jak i czek agencji lokalnej lub

Kontrola Agencji Narodowej (LAC/NAC) oraz „Konieczne informacje" mogą być wymagane na wyższym poziomie.

* Uzyskuje klucz publiczny subskrybenta od subskrybenta.

* Dostarcza subskrybentowi klucz publiczny CA. Kotwica zaufania to klucz publiczny urzędu certyfikacji, któremu ufa strona ufająca. Zaufanie to zazwyczaj jest ustanawiane przez uzyskanie klucza publicznego z zaufanego źródła za pomocą zaufanych środków, takich jak fizyczne przekazanie lub za pośrednictwem protokołu Secure Sockets Layer (SSL) z zaufanej lub znanej witryny internetowej. Klucz publiczny urzędu certyfikacji staje się kotwicą zaufania subskrybenta.

* Wysyła żądanie utworzenia certyfikatu do urzędu certyfikacji. Zazwyczaj RA tworzy wiadomość poczty elektronicznej zawierającą nazwę subskrybenta i klucz publiczny subskrybenta, podpisuje cyfrowo wiadomość i wysyła wiadomość do urzędu certyfikacji. Inne środki transportu, takie jak podręcznik lub Internet, również są odpowiednie, o ile istnieje pewność, że tożsamość subskrybenta i klucz publiczny nie zostaną zmienione. Standard X.509 nie określa protokołu dla żądań generowania certyfikatów. Grupa robocza Infrastruktury Klucza Publicznego dla certyfikatu X.509 (PKIX) grupy roboczej IETF (Internet Engineering Task Force) opracowała standardy internetowe w tym zakresie

POLITYKA CERTYFIKATÓW

Aby zapewnić bezpieczeństwo PKI, komponenty PKI muszą działać z wysokim stopniem bezpieczeństwa. Aby to zapewnić:

* Klucze prywatne muszą być traktowane jako poufne.

* Klucze prywatne mogą być używane tylko przez właścicieli kluczy.

* Należy zapewnić integralność klucza publicznego kotwic zaufania.

* Wstępne uwierzytelnienie subskrybenta (posiadacza klucza prywatnego i podmiotu certyfikatu klucza publicznego) musi być silne, aby kradzież tożsamości nie wystąpiła w momencie tworzenia certyfikatu.

* Systemy i aplikacje komputerowe CA i RA muszą być chronione przed manipulacją.

* Wymagania dotyczące poziomu zaufania muszą być jasno określone

Polityka Certyfikacji (CP) musi szczegółowo określać zawartość certyfikatu, zarówno pola, jak i rozszerzenia. Wszystko, co jest nieobecne w CP, nie powinno znajdować się w certyfikacie. Oprócz wymogów bezpieczeństwa oraz w celu ułatwienia handlu elektronicznego, PKI musi uwzględniać zobowiązania wszystkich stron i ich odpowiedzialność w przypadku sporu. Te kwestie bezpieczeństwa,

odpowiedzialności, poziomu zaufania i zobowiązań są wyartykułowane w CP. Zgodnie ze standardem X.509, CP to „nazwany zestaw reguł, który wskazuje zastosowanie certyfikatu do określonej społeczności i/lub klasy aplikacji o powszechnych wymaganiach bezpieczeństwa”.6 Użytkownik certyfikatu może użyć CP do podjęcia decyzji czy certyfikat i wiążące wiązanie między certyfikatem a jego właścicielem są wystarczająco godne zaufania dla określonej aplikacji. Punkt kontrolny dotyczy bezpieczeństwa i obowiązków wszystkich komponentów PKI, nie tylko urzędu certyfikacji; obejmuje to CA, RA, repozytorium, subskrybenta i stronę ufającą. Bardziej szczegółowy opis praktyk stosowanych przez urząd certyfikacji przy wydawaniu certyfikatów i zarządzaniu nimi znajduje się w oświadczeniu o praktykach certyfikacyjnych (CPS) opublikowanym przez urząd certyfikacji lub do którego się odwołuje. Zgodnie z wytycznymi American Bar Association’s Digital Signature Guidelines (zwanymi dalej „ABAGuidelines”) „CPS to oświadczenie praktyk stosowanych przez urząd certyfikacji przy wydawaniu certyfikatów.” Chociaż CP i CPS oba dotyczą tych samych tematów, CP określa wymagania bezpieczeństwa i zobowiązania dla PKI przedsiębiorstwa, a CPS opisuje, w jaki sposób te wymagania są spełniane przez PKI przedsiębiorstwa. CP i CPS są również używane inaczej. CP stanowi podstawę dla certyfikacji krzyżowej ponad granicami przedsiębiorstwa w celu ułatwienia bezpiecznej, elektronicznej komunikacji między przedsiębiorstwami . Identyfikator obiektu (OID) wskazujący na CP (który może być Universal Resource Locator [URL]) jest używany do tworzenia certyfikatu, który można umieścić w rozszerzeniu „Polityki certyfikatów” certyfikatów X.509. W ten sposób OID umożliwia stronom ufającym zapoznanie się z dbałością złożoną podczas generowania certyfikatów, zalecanym użytkowaniem i obowiązkami różnych stron. Ponieważ certyfikaty mogą być tworzone z różnymi poziomami zaufania i mogą być oparte na oprogramowaniu lub sprzęcie (bardziej bezpieczne), często rozszerzenie „Zasady certyfikatów” jest jedynym wskaźnikiem poziomu zaufania, który powinien być umieszczony w certyfikacie. CPS umożliwia personelowi PKI korzystanie z komponentów PKI i administrowanie nimi. CPS stanowi również podstawę audytów zgodności w celu zapewnienia, że komponenty PKI działają zgodnie z postanowieniami CPS. Rysunek 37.5 ilustruje elementy kompleksowego CPS. Komponenty dzielą się dalej na podkomponenty, które z kolei dzielą się na elementy. Komponenty mogą być odpowiednie dla różnych jednostek PKI, ale mogą być stosowane w ten sam lub inny sposób. Na przykład techniczne środki bezpieczeństwa mogą dotyczyć CA, RA, subskrybentów i stron ufających. Kontrole te mogą być różne dla każdego z tych podmiotów, przy czym najbardziej rygorystyczne są dla urzędu certyfikacji, następnie RA, a następnie subskrybentów i stron ufających.

GLOBALNA INFRASTRUKTURA KLUCZU PUBLICZNEGO

Zasady korporacyjnej infrastruktury PKI z jednym urzędem certyfikacji można rozszerzyć w celu obsługi globalnego, bezpiecznego handlu elektronicznego, opierając się na wielu urzędach certyfikacji i/lub urzędach certyfikacji w celu certyfikacji innych urzędów certyfikacji i siebie nawzajem. Sposób wzajemnej certyfikacji przez urzędy certyfikacji jest również nazywany modelem zaufania, wykresem zaufania lub architekturą PKI. Aby jedna osoba mogła bezpiecznie komunikować się z drugą, musi istnieć ścieżka zaufania od kotwic zaufania strony ufającej do subskrybenta, którego podpis musi zostać zweryfikowany lub do którego ma zostać wysłana zaszyfrowana wiadomość.

Poziomy zaufania

Jak wspomniano w dokumencie Office of Manpower and Budget Memorandum OMB M04-04, sekcja 2.1, istnieją cztery podstawowe poziomy zaufania:

Poziom 1. Niewielkie zaufanie do potwierdzanej tożsamości lub brak pewności

Poziom 2. Pewna wiara w słuszność stwierdzonej tożsamości

Poziom 3. Wysoka pewność co do słuszności stwierdzonej tożsamości

Poziom 4. Bardzo wysoka pewność słuszności stwierdzonej tożsamości

Każdy poziom wymaga innego początkowego uwierzytelnienia tożsamości, a wyższe poziomy (lub te używane do informacji niejawnych) wymagają dochodzenia w tle. Poziom 3 jest również znany jako Medium Assurance i dzieli się na dwie formy: (1) oprogramowanie (certyfikaty i klucze można eksportować i przenosić między urządzeniami) oraz (2) sprzęt (certyfikaty można eksportować, ale klucze i funkcje kryptograficzne są wykonywane na określone urządzenie sprzętowe [np. karta inteligentna, token USB lub urządzenie PC-Card]). Większość komercyjnych PKI wykorzystuje odpowiednik średniego poziomu pewności.

Sprawdzenie

Każdy poziom pewności ma wymóg sprawdzania (znany również jako weryfikacja), który rośnie wraz z poziomem zaufania, jak pokazano na Rysunku 37.7. Zasadniczo żaden nie jest wymagany na poziomie 1 (podstawowym), podczas gdy na poziomie 4 (wysokim) istnieją obszerne wymagania osobiste.

Zaufane ścieżki

Model zaufania może być postrzegany jako łańcuch, którego ogonem jest urząd certyfikacji wystawiający certyfikat, a jego głową jest subskrybent (tj. podmiot certyfikatu). Subskrybentem może być inny urząd certyfikacji lub podmiot końcowy. Aby potwierdzić wiarygodność certyfikatu, należy zacząć od kotwicy zaufania strony ufającej i podążać w kierunku łańcucha, aż do osiągnięcia subskrybenta (zainteresowanego stroną ufającą). Globalna bezpieczna komunikacja wymaga, aby istniała ścieżka zaufania od każdego abonenta do każdego innego abonenta. Strona ufająca może zacząć od swojej kotwicy zaufania i zweryfikować certyfikaty wystawione przez kotwicę zaufania. Gdy tak się stanie, można zaufać kluczom publicznym i wykorzystać je do weryfikacji certyfikatów wydanych przez te urzędy certyfikacji. Może to być wykonywane rekursywnie przez stronę ufającą do momentu zweryfikowania certyfikatu klucza publicznego zainteresowanego subskrybenta. Następnie klucz publiczny subskrybenta może służyć do weryfikacji podpisów cyfrowych oraz do wykonania szyfrowania.

Modele zaufania

Przykłady modeli zaufania w ramach PKI, które odnoszą się do zaufania do certyfikatu i różnią się od weryfikacji (zaufania tożsamości), obejmują:

* Ścisła hierarchia

* Hierarchia

* Most

* Wiele kotwic zaufania

* Siatka (aka anarchia lub sieć)

* Kombinacja

Ścisła hierarchia

Dowód ilustruje ścisłą hierarchię. Jest to struktura drzewiasta z jednym korzeniem. W ścisłej hierarchii, aby komunikować się z dwiema stronami nawzajem, wymagają klucza publicznego ich wspólnego przodka jako kotwicy zaufania. Weryfikowalne łańcuchy certyfikatów wymagają, aby strony miały

wspólnego przodka. Aby wszystkie strony mogły bezpiecznie komunikować się ze sobą, jako kotwica zaufania wymagany jest pojedynczy root, ponieważ jest to jedyna wspólna kotwica zaufania.

Hierarchia

W (nieścisłej) hierarchii podrzędne urzędy certyfikacji certyfikują swoich rodziców. Ponieważ graf skierowany jest dwukierunkowy, każdy urząd certyfikacji może być kotwicą zaufania dla stron uzależnionych. Jednak z praktycznego, operacyjnego i wydajnościowego punktu widzenia (tj. długości ścieżki certyfikatu) lokalny urząd certyfikacji powinien być kotwicą zaufania. Lokalny urząd certyfikacji to urząd certyfikacji, który wystawił certyfikat stronie ufającej.

Most

Kolejnym modelem zaufania jest most. W tym modelu jeden urząd certyfikacji przeprowadza krzyżową certyfikację z każdym urzędem certyfikacji z różnych domen. Domeną mogą być organizacje lub segmenty wertykalne, takie jak bankowość lub opieka zdrowotna. Pomost CA nie jest kotwicą zaufania dla żadnej strony ufającej. CA w domenie strony ufającej jest kotwicą zaufania. W domenie nie ma ograniczeń dotyczących modelu zaufania. Sama domena PKI może być zorganizowana jako dowolny z zaufanych modeli, w tym mostu, co prowadzi do możliwych warstw urzędów certyfikacji mostu.

Wiele kotwic zaufania

Inną alternatywą jest uzyskanie przez stronę ufającą kluczy publicznych różnych urzędów certyfikacji w zaufany sposób, a następnie użycie tych kluczy publicznych jako kotwic zaufania. Takie podejście jest atrakcyjne, gdy urzędy certyfikacji nie mogą lub nie chcą przeprowadzać certyfikacji krzyżowej, a strona ufająca musi bezpiecznie komunikować się z subskrybentami w domenach urzędów certyfikacji, z których pochodzą. Takie podejście nazywa się wieloma kotwicami zaufania. Każda kotwica zaufania reprezentująca domenę może być pojedynczym urzędem certyfikacji lub PKI z kolekcją urzędów certyfikacji w modelu zaufania.

Siatka

Ostatnim przykładem modelu zaufania jest siatka (inaczej sieć lub anarchia). Termin „siatka” opisuje dowolny obraz reprezentujący zaufanie między urzędami certyfikacji lub certyfikatami bez żadnych określonych reguł lub wzorców. Model ten jest czasem nazywany siecią zaufania i jest szczególnie kojarzony z oryginalnym projektem Pretty Good Privacy, jednym z pierwszych popularnych systemów implementujących certyfikaty klucza publicznego. W ramach tej struktury każdy odbiorca musi wyraźnie ufać sobie nawzajem. Głównym problemem jest to, że nie skaluje się zbyt dobrze poza kilkuset użytkowników.

Wybór architektury infrastruktury klucza publicznego

To, czy domena (przedsiębiorstwo) wybierze jeden urząd certyfikacji, czy wiele urzędów certyfikacji do swojej operacji wewnątrzdomenowej, należy określić na podstawie różnych czynników, w tym:

* Kultura zarządzania

* Polityka organizacji

* Rozmiar ścieżki certyfikacji

* Wielkość populacji subskrybenta

* Rozkład populacji subskrybentów

* Informacje o odwołaniu

W wielu sytuacjach polityka lub struktura zarządzania może dyktować istnienie wielu urzędów certyfikacji w domenie. Innymi słowy, organizacje na poziomie jednostki biznesowej, na poziomie biura regionalnego, na poziomie korporacji lub na poziomie krajowym mogą chcieć stworzyć CA, aby zapewnić im pewien stopień kontroli, niezależności, autonomii i prestiżu. Sposób organizacji tych urzędów certyfikacji (dwustronna certyfikacja krzyżowa, hierarchia itp.) będzie również zależeć od zarządzania i krajobrazu politycznego domeny. Model zaufania powinien być taki, aby umożliwiał zarządzanie rozmiarem ścieżki certyfikacji; w przeciwnym razie użytkownicy końcowi zobaczą niedopuszczalne pogorszenie wydajności uzyskiwania certyfikatów i list CRL oraz weryfikowania podpisów cyfrowych na certyfikatach i listach CRL. Podobnie, duże populacje subskrybentów mogą wymagać więcej niż jednego urzędu certyfikacji, aby zapewnić, że urząd certyfikacji może zarządzać subskrybentami i utrzymać mały rozmiar listy CRL. W przypadku wybrania produktów urzędu certyfikacji, które wystawiają partycjonowane listy CRL, można zarządzać rozmiarami list CRL nawet w przypadku bardzo dużej populacji subskrybentów. Rozważając międzydomenową certyfikację krzyżową, należy wziąć pod uwagę podobne kwestie.

Certyfikacja krzyżowa

W najprostszej formie certyfikacja krzyżowa składa się z dwóch urzędów certyfikacji, które certyfikują się wzajemnie, wydając sobie nawzajem certyfikat. Certyfikaty mogą być przechowywane w określonych atrybutach wpisu do katalogu w certyfikacie; przykłady obejmują parę atrybutów cross-certificate lub certyfikat CA. Z certyfikacją krzyżową wiążą się dwa praktyczne problemy. Jeden zajmuje się produktami handlowymi. Jeśli te dwie domeny korzystają z różnych produktów, ich urzędy certyfikacji mogą nie być w stanie wymieniać informacji w celu przeprowadzenia certyfikacji krzyżowej, a ich katalogi mogą nie być w stanie połączyć w łańcuch, aby umożliwić stronom ufającym pobieranie certyfikatów.

Drugi problem jest operacyjny. Przed certyfikacją innego urzędu certyfikacji, urząd certyfikacji wystawiający certyfikat musi upewnić się, że przedmiotowy urząd certyfikacji działa zgodnie z akceptowanymi mechanizmami kontroli, określonymi w CP. Wystawiający urząd certyfikacji potwierdza odpowiedni CP w rozszerzeniu „polityki certyfikatów" certyfikatu X.509 w wersji 3 przedmiotowego urzędu certyfikacji. W praktyce oba CA przeprowadzają wzajemne poświadczenie wzajemnej certyfikacji po dokonaniu wzajemnego przeglądu swoich CP i po upewnieniu się, że CP można uznać za równoważne. Nie oznacza to, że wszystkie kontrole bezpieczeństwa i obowiązki są identyczne, ale muszą oferować w przybliżeniu podobne poziomy zaufania i zobowiązań oraz podobną odpowiedzialność i ulgę finansową. Gdy dwa urzędy certyfikacji przeprowadzają wzajemne certyfikację krzyżową, zaufanie na ogół dotyczy ograniczonego zestawu zasad poprzez potwierdzenia w rozszerzeniach „zasad certyfikatów", a zaufanie jest tylko dwustronne. Innymi słowy, zaufanie nie zmieni się; pozostanie między dwoma urzędami certyfikacji. Urzędy certyfikacji zapewniają to poprzez hamowanie mapowania polityki poprzez rozszerzenie „policy limits". Rozszerzenia ograniczeń zasad umożliwiają różne zahamowania mapowania zasad w łańcuchu certyfikatów. W większości bezpośrednich certyfikacji krzyżowych mapowanie zasad powinno zostać natychmiast wstrzymane. W przypadku certyfikacji krzyżowej z wykorzystaniem modelu pomostowego CA, aby skorzystać z usług mapowania polityk pomostowego CA, inhibicja polisy powinna być inna dla jednego certyfikatu (czyli certyfikatu pomostowego CA). Ponadto oba urzędy certyfikacji powinny używać rozszerzenia „ograniczenia nazw" w certyfikatach X.509 w wersji 3, aby upewnić się, że ufają drugiej domenie w zakresie nazw, nad którymi ta druga ma kontrolę. Korzystanie z tego rozszerzenia minimalizuje również szanse na kolizję nazw. W przypadku dwustronnej certyfikacji krzyżowej mapowanie polityk powinno zostać natychmiast wstrzymane przez użycie wartości „0" w polu „inhibit policy mapping" rozszerzenia

ograniczeń polityk w certyfikatach X.509. Gdy pomost CA jest używany do interoperacyjności międzydomenowej, w tym polu należy użyć wartości „1”. Pozwoli to domenie wydającego urzędu certyfikacji na mapowanie swoich zasad do zasad pomostowego urzędu certyfikacji, a następnie zezwoli pomostowemu urzędowi certyfikacji na mapowanie swoich zasad na przedmiotową domenę urzędu certyfikacji, w efekcie mapowanie z domeny wydającego urzędu certyfikacji na domenę przedmiotowego urzędu certyfikacji. Dopóki wystawiający urząd certyfikacji używa swojej kontroli nad mapowaniem zasad blokowania, pomostowy urząd certyfikacji nie musi używać mapowania zasad blokowania do kontrolowania blokowania mapowania.

Interoperacyjność infrastruktury klucza publicznego

Złożoność technologii, standardów i produktów technologii PKI z jednej domeny do drugiej iz jednego produktu do drugiego czasami stwarza problemy z interoperacyjnością. Jednak bez interoperacyjności międzydomenowej nie może istnieć zaufanie globalne, a jedynie zaufanie indywidualne. Czynniki te odgrywają kluczową rolę w zapewnieniu interoperacyjności PKI:

* Ścieżka zaufania

* Algorytmy kryptograficzne

*Formaty certyfikatów i listy CRL

* Rozpowszechnianie certyfikatów i list CRL

* Zasady dotyczące certyfikatów

* Nazwy

Ścieżka zaufania

Strony komunikujące się muszą być w stanie utworzyć ścieżki zaufania od swoich kotwic zaufania do swoich subskrybentów. Można to osiągnąć za pomocą wielu kotwic zaufania, certyfikacji krzyżowej i innych opisanych wcześniej modeli zaufania.

Algorytmy kryptograficzne.

Strony komunikujące się muszą wdrożyć stosowane przez siebie algorytmy kryptograficzne, takie jak hashowanie, podpisy cyfrowe, szyfrowanie kluczy i szyfrowanie danych. Ponadto strony powinny mieć możliwość komunikowania się ze sobą algorytmów, których używają. W certyfikatach X.509 i CRL informacje te mogą być zawarte w samych obiektach, podobnie jak w polu algorytmu. W certyfikatach X.509 dla przekazywanych informacji algorytmy, takie jak podpis cyfrowy i algorytm szyfrowania klucza, mogą być przenoszone w certyfikacie podmiotu końcowego. Algorytm mieszający i algorytm szyfrowania danych mogą stanowić część dorozumianej umowy między stronami lub mogą być przenoszone wraz z przekazywanymi informacjami. Informacje można również uzyskać z obsługiwanego atrybutu algorytmów wpisu katalogu X.500 użytkownika, chociaż ta opcja nie jest powszechnie stosowana. Chociaż oczekiwane algorytmy klucza publicznego używane przez CA do tworzenia certyfikatu muszą być rozpoznawalne przez odbiorcę (w celu zrozumienia zawartości certyfikatu), ważne jest, aby certyfikat nie zawierał żadnych asercji co do algorytmów symetrycznych, które mogą być użyte. Certyfikat powinien być niezależny od aplikacji i nie nakładać żadnych reguł na aplikacje, gdy nie jest to konieczne. We wszystkich tych sytuacjach algorytm jest identyfikowany za pomocą identyfikatorów obiektów. Różne organizacje mogą zarejestrować ten sam algorytm pod swoim łukiem OID. Dlatego ważne jest, aby albo te dwie domeny używały tego samego OID dla algorytmów, albo aby ich oprogramowanie interpretowało wiele OID jako ten sam algorytm. Z tego

powodu proliferacja OID dla algorytmów nie jest zalecana. Warianty tego samego algorytmu podstawowego dodatkowo pogłębiają problemy z interoperacyjnością algorytmów. Na przykład, subtelne dopełnienie i inne różnice istnieją między definicjami algorytmu RSA w Standardach Kryptografii Klucza Publicznego (PKCS) i w komitecie X9 Amerykańskiego Narodowego Instytutu Standardów (ANSI). Podobnie algorytm Diffie-Hellmana ma różne tryby i różne sposoby redukcji obliczonego klucza tajnego do rozmiaru klucza symetrycznego (tj. sposoby zmniejszania kluczy sesji). Każda z tych różnic w algorytmach musi być udokumentowana za pomocą różnych OID, aby OID wywołał odpowiednią implementację. Ważne jest, aby rozszerzenia były wybierane ostrożnie. Te dotyczące algorytmów często mają znaczenie w kontekście konkretnej aplikacji. Jak wspomniano wcześniej, dobrym przykładem rozszerzenia, którego nie należy umieszczać w certyfikacie, jest rozszerzenie SMIME Capabilities, ponieważ nie określa ono minimalnych oczekiwań, a zamiast tego może ograniczać długość klucza symetrycznego, którego mogą używać aplikacje. Takie rozszerzenia specyficzne dla aplikacji należy unikać w certyfikatach użytkownika/subskrybenta. Algorytmy i długości kluczy używane przez elementy klucza publicznego (asymetryczne) są określone w wartościach pola, takich jak Informacje o kluczu publicznym podmiotu.

Format certyfikatu i listy unieważnionych certyfikatów

Strony komunikujące się muszą współdzielić lub muszą być w stanie zrozumieć nawzajem swoje certyfikaty i formaty listy CRL. Najczęstszym sposobem osiągnięcia tego jest użycie wspólnego standardu, takiego jak X.509. Wiele razy było to niewystarczające ze względu na niejednoznaczność standardu i powiązanych schematów kodowania, chociaż z biegiem czasu błędy te zostały naprawione. Obecnie głównym powodem, dla którego certyfikaty i listy CRL wydawane przez jeden produkt mogą nie być rozumiane przez inny, jest to, że jeden lub oba nie są zgodne z normą lub jeden produkt nie realizuje wszystkich cech normy stosowanej przez inny produkt. Strony komunikujące się muszą uzyskać certyfikaty i listy CRL wydane przez różne urzędy certyfikacji w swoich domenach. Te certyfikaty i listy CRL można uzyskać z repozytorium, takiego jak serwer X.500 i Lightweight Directory Access Protocol (LDAP). Alternatywnie, certyfikaty i listy CRL mogą być przenoszone jako część protokołu komunikacyjnego między stronami, na przykład zgodnie z definicją w S/MIME (Secure/Multipurpose Internet Mail Extension) w wersji 3. Repozytoria X.500 i LDAP są oparte na hierarchii bazy danych. Każdy węzeł w hierarchicznej strukturze drzewa należy do klasy obiektów. Klasa obiektu węzła określa atrybuty, które są przechowywane dla tego węzła. Przykładami atrybutów są stanowisko, numer telefonu, numer faksu i tym podobne. Certyfikaty i listy CRL są również atrybutami. X.500 i LDAP zdefiniowały standardowy schemat dla certyfikatów PKI i list CRL. W przypadku certyfikatów te atrybuty to userCertificate, cACertificate i crossCertificatePair. Certyfikaty jednostki końcowej powinny być przechowywane w atrybucie userCertificate. Wszystkie certyfikaty CA powinny być przechowywane w elemencie forward atrybutu crossCertificatePair podmiotu CA. Ponadto wszystkie certyfikaty wydane urzędom certyfikacji w tej samej domenie powinny być przechowywane w atrybucie cACertificate podmiotu CA. Różne listy odwołania powinny być przechowywane w atrybutach cRL, aRL i deltaCRL wystawiającego urzędu certyfikacji, stosownie do przypadku. Jeśli certyfikaty i listy CRL nie są przechowywane w tych ustandaryzowanych atrybutach, oprogramowanie strony zależnej może nie być w stanie uzyskać tych obiektów. Ponadto produkty katalogowe X.500 nadal mogą nie zawsze współpracować ze względu na dodatkową złożoność standardu X.500 i różnice między produktami. Wdrażając katalogi X.500 i łącząc produkty katalogowe X.500 od różnych dostawców, realizatorzy powinni mieć czas na współdziałanie produktów i katalogów.

Zasady certyfikacji

W celu wzajemnego zaufania i wzajemnej certyfikacji urzędy certyfikacji w dwóch domenach muszą działać zgodnie z podobnymi zasadami. Użytkownicy w dwóch domenach powinni mieć możliwość

akceptowania lub odrzucania certyfikatów ze swoich domen na podstawie wymagań bezpieczeństwa aplikacji oraz zasad, zgodnie z którymi certyfikaty zostały wydane. W celu określenia podobieństwa lub równoważności polityk obu domen, CP powinien być napisany przy użyciu standardu IETF RFC-2527. CP jest reprezentowany za pomocą OID w certyfikacie. Aby upewnić się, że oprogramowanie użytkownika akceptuje i odrzuca certyfikaty na podstawie wymagań aplikacji i CP, produkty PKI powinny być wybierane i konfigurowane w taki sposób, aby urząd certyfikacji odpowiednio potwierdzał zasady certyfikatów, mapowanie zasad i rozszerzenia ograniczeń zasad. Oprogramowanie użytkownika obsługujące PKI musi przetwarzać te rozszerzenia odpowiednio iw pełni zgodnie z wymaganiami reguł weryfikacji ścieżki certyfikatu X.509.

Nazwy

Domeny komunikujące się nie mogą przypisywać tej samej nazwy dwóm różnym podmiotom. Nazwy wyróżniające (DN) X.500 to kroki w tym kierunku, ale niewystarczające do osiągnięcia tego celu. Aby zilustrować tę kwestię, rozważmy na przykład CygnaCom, spółkę zarejestrowaną we Wspólnocie Wirginii. Chociaż jest bardzo mało prawdopodobne, że w Wirginii istnieje inny CygnaCom, nie ma pewności, że nie ma CygnaCom zarejestrowanego w innych stanach USA. W ten sposób byłoby możliwe, że c=US, O=CygnaCom mogą zostać potwierdzone przez urzędy certyfikacji dla kilku różnych domen. Aby uniknąć kolizji nazw i niejednoznaczności, należy użyć rozszerzenia ograniczeń nazw w X.509. CA dla jednej domeny może uniemożliwić innym podmiotom używanie nazwy zarejestrowanej w tej domenie. Urząd certyfikacji (CA „Y" w tym przykładzie) używa rozszerzenia ograniczeń nazw, aby zapewnić priorytet i kontrolę nad określonym identyfikatorem. Na przykład pierwszy urząd certyfikacji, który certyfikuje firmę o nazwie CygnaCom w swojej domenie, powinien ustawić atrybut ograniczenia nazwy w swoim certyfikacie dla swojego CygnaCom, stwierdzając, że tylko jego CygnaCom może wydawać certyfikaty w przestrzeni nazw c=US, O=CygnaCom. Gdyby pojawił się inny CygnaCom, CA „Y" poprosiłby drugiego CygnaComa o wybranie innej nazwy, aby uniknąć kolizji nazw. Chociaż ten przykład koncentruje się na nazwie DN, ograniczenie nazwy może być używane dla dowolnych hierarchicznych form nazw, w tym nazwy DN, nazw zgodnych z RFC 822 i innych. Produkty PKI powinny być wybierane i konfigurowane tak, aby urząd certyfikacji odpowiednio potwierdzał rozszerzenie ograniczeń nazw. Oprogramowanie użytkownika obsługujące PKI musi przetwarzać to rozszerzenie odpowiednio iw pełni zgodnie z wymaganiami reguł weryfikacji ścieżki certyfikatu X.509.

FORMY ODWOŁANIA

Jak omówiono wcześniej, PKI zawiera mechanizmy odwoływania kluczy. Niezbędne jest ustanowienie przepisów dotyczących unieważniania skompromitowanych kluczy w celu utrzymania relacji zaufania dowolnej infrastruktury PKI stosowanej w środowisku rzeczywistym. Pierwszą zaprojektowaną formą unieważnienia była lista CRL. Wydaje się ,że to najbardziej odpowiednia forma odwołania, biorąc pod uwagę rozproszone ramy uwierzytelniania PKI. Mechanizm CRL umożliwia CA generowanie obiektów, a stronom zależnym bezpieczne ich przetwarzanie bez martwienia się o bezpieczeństwo serwerów lub systemu dostarczającego listę CRL oraz bez obaw o sieć (sieci), przez którą przechodzi CRL.

Rodzaje mechanizmów powiadamiania o unieważnieniu

Jednak pojawiło się kilka obaw dotyczących listy CRL, które doprowadziły do powstania innych form mechanizmów powiadamiania o unieważnieniu. Wiele z tych mechanizmów to odmiany listy CRL w tym sensie, że są to listy odwołania, ale nie są one kompletne. Druga kategoria mechanizmów odwołania odracza przetwarzanie informacji o odwołaniu do serwera, na przykład za pośrednictwem protokołu OCSP (Online Certificate Status Protocol); . Trzecia kategoria mechanizmów pozwala użytkownikom sprawdzić status pojedynczego certyfikatu z katalogu i umożliwia urzędu certyfikacji aktualizowanie stanu tego certyfikatu w katalogu. Ostatnia kategoria pozwala urządowi certyfikacji lub

innemu zaufanemu serwerowi zorganizować informacje o odwołaniu w B-drzewie. Wybór mechanizmu lub mechanizmów zależy od wielu czynników, takich jak:

* Model komunikacji (tj. jaka klasa użytkowników komunikuje się z jaką inną klasą). Na przykład, jeśli użytkownik komunikuje się z kilkoma użytkownikami, którzy są subskrybentami tego samego urzędu certyfikacji, pojedyncza lista CRL z tego urzędu certyfikacji zapewni odpowiednie informacje o wszystkich docelowych użytkownikach. Jeśli użytkownik komunikuje się z użytkownikami należącymi do różnych urzędów certyfikacji, każda lista CRL zawiera informacje o tylko jednym użytkowniku.

* Architektura katalogów: gdzie się znajdują i które części informacji katalogowych są replikowane lub ukryte?

* Dostępna przepustowość komunikacji.

* Czas wiązania (tj. czas na nawiązanie połączenia z repozytorium w celu wykonania pobierania i aktualizacji) w celu uzyskania dostępu do repozytorium.

* Rozmiar odpowiedzi o unieważnieniu z repozytorium (np. rozmiar listy CRL).

* Obciążenie przetwarzania repozytorium, zwłaszcza w przypadku generowania podpisów cyfrowych na informacjach o odwołaniu.

* Obciążenie przetwarzania na stacji roboczej użytkownika, zwłaszcza w przypadku weryfikacji podpisu cyfrowego na informacjach o unieważnieniu.

Listy unieważnionych certyfikatów i ich warianty

Pierwszy zestaw mechanizmów, lista CRL i jej różne formy, jest najbardziej wszechstronnym, skutecznym i zalecanym podejściem do powiadamiania o unieważnieniu. Podobnie jak certyfikaty X.509, listy CRL są wyrażone w formacie ASN.1. Istnieje kilka podstawowych typów list CRL i należy je dokładnie rozważyć, w oparciu o model komunikacji z użytkownikiem i przewidywany wskaźnik odwołania:

* Pełna i kompletna lista CRL

* Lista odwołania urzędu (ARL)

* CRL punktu dystrybucji

* Delta CRL

Pełna i kompletna lista CRL

Pełna i kompletna lista CRL to lista CRL zawierająca informacje o unieważnieniu wszystkich certyfikatów wystawionych przez urząd certyfikacji. Ten typ listy CRL jest rzadko spotykany; zamiast tego zwykła lista CRL zawiera tylko informacje o unieważnionych certyfikatach, a nie o aktualnie ważnych. Wygasłe certyfikaty nie są uwzględniane, a unieważnione certyfikaty po wygaśnięciu zostaną usunięte z listy CRL.

Lista Uprawnień do Odwołania

ARL to lista CRL zawierająca informacje o unieważnieniu wszystkich certyfikatów CA wystawionych przez CA; oznacza to, że lista ARL jest podzbiorem listy CRL dla certyfikatów wystawionych tylko dla urzędów certyfikacji. ARL jest bardzo pożądanym mechanizmem z tych powodów:

* Prawdopodobnie będzie krótki. CA prawdopodobnie certyfikuje mniej CA niż inne typy subskrybentów. Ponadto, biorąc pod uwagę, że urzędy certyfikacji mają działać z dużą ostrożnością i biorąc pod uwagę, że urzędy certyfikacji nie będą odwoływane z powodów takich jak zmiana nazwy lub zmiana przynależności organizacyjnej, urzędy certyfikacji będą odwoływane znacznie rzadziej niż jednostki końcowe. Te czynniki przyczynią się do bardzo małego ARL.

* W przypadku wszystkich certyfikatów z wyjątkiem jednego należy sprawdzić tylko ARL, ponieważ w ścieżce certyfikatu wszystkie certyfikaty oprócz ostatniego są wydawane do urzędu certyfikacji.

Ze względu na lukę bezpieczeństwa w X.509 w wersji 1 urząd certyfikacji nigdy nie powinien wystawiać ARL zdefiniowanych przy użyciu tej wersji. W X.509 w wersji 1 nie ma różnicy między formatem CRL a formatem ARL. Ponieważ zarówno listy CRL, jak i ARL są podpisywane przez ten sam urząd certyfikacji, gdyby przeciwnik (adwersarz katalogowy lub sieciowy) dostarczył ARL stronie ufnej zamiast pełnej listy CRL, strona ufająca nie miałaby możliwości dowiedzenia się, że otrzymała ARL zamiast żądanej listy CRL. ARL nie zawierałby informacji o odwołaniu podmiotu końcowego, a zatem mógłby wprowadzić w błąd stronę ufającą do korzystania z unieważnionego certyfikatu podmiotu końcowego. Protokół ARL X.509 w wersji 2 naprawia tę lukę w zabezpieczeniach za pomocą rozszerzenia punktu dystrybucji wydającego. ARL musi używać tego rozszerzenia i potwierdzać pole, które stwierdza, że lista zawiera tylko certyfikaty CA. Obecność tego pola w podpisanej liście ARL informuje stronę ufającą, że nie jest to pełna lista CRL. Teraz, gdyby przeciwnik dostarczył ARL zamiast CRL, strona ufająca wykryłaby to podstawienie za pomocą pola wystawiającego punktu dystrybucji. Jest to jeden z kilku powodów bezpieczeństwa, dla których oprogramowanie obsługujące PKI musi być w stanie prawidłowo przetwarzać różne rozszerzenia zgodnie z wymaganiami określonymi w standardzie X.509.

Lista CRL punktu dystrybucji

Lista CRL punktu dystrybucji to mechanizm, który posiada kilka przydatnych funkcji:

* Aby zreplikować listę CRL

* Aby skonsolidować informacje o unieważnieniach z różnych CA, tak aby strony ufające musiały uzyskać tylko jedną listę CRL

* Aby podzielić informacje o unieważnieniu dla subskrybentów urzędu certyfikacji na wiele mniejszych części

Ta ostatnia funkcja, partycja, jest osiągana przez zapewnienie rozszerzenia punktu dystrybucji listy CRL w certyfikacie, który wskazuje na wpis nazwy, pod którym będą wyświetlane informacje o odwołaniu certyfikatu. Partycjonowana lista CRL będzie potwierdzać tę samą nazwę w polu Punkt dystrybucji rozszerzenia punktu dystrybucji wystawiającego na liście CRL. Ponieważ wszystkie partycjonowane listy CRL (punktu dystrybucji) są podpisane przez ten sam urząd certyfikacji, nie wystarczy, aby strona ufająca po prostu zweryfikowała podpis urzędu certyfikacji na liście CRL punktu dystrybucji. Strona uzależniona musi być zgodna z nazwą punktu dystrybucji w rozszerzeniu punktu dystrybucji na liście CRL z nazwą punktu dystrybucji w rozszerzeniu punktu dystrybucji w certyfikacie.

Lista unieważnionych certyfikatów Delta

Jeszcze innym sposobem zmniejszenia rozmiaru listy CRL jest opublikowanie zmian informacji o odwołaniu od ostatniej listy CRL. Lista CRL zawierająca tylko zmiany jest nazywana różnicową listą CRL, a lista CRL, na której publikowane są zmiany, jest nazywana podstawową listą CRL. Różnicową listę CRL można zastosować do dowolnej z następujących list CRL: CRL, ARL i CRL punktu dystrybucji. W celu skonstruowania aktualnych informacji o odwołaniu należy użyć najnowszej delta CRL i jej bazy. Istnieje

algorytm, którego można użyć, aby umożliwić zastosowanie podzbioru zmian do wcześniejszej listy CRL, która nadal będzie pasować do podpisu cyfrowego nowej listy CRL.

Protokoły odwołania oparte na serwerze

Odwoływanie na serwerze wykorzystuje protokoły, takie jak protokół stanu certyfikatu on-line (OCSP) i prosty protokół sprawdzania poprawności certyfikatu (SCVP). Ogólnie rzecz biorąc, protokoły te mają kilka wad, w tym te:

* Ponieważ informacje o odwołaniu są tworzone na serwerze, kanał komunikacji między stroną ufającą a serwerem musi być zabezpieczony, najprawdopodobniej za pomocą podpisów cyfrowych.

* Podpisane operacje ograniczą skalowalność serwera, ponieważ generowanie podpisów cyfrowych wymaga dużej mocy obliczeniowej.

* Ponieważ informacje o odwołaniu są tworzone na serwerze, schemat wymaga zaufanego serwera w przeciwieństwie do niezaufanego repozytorium

* Odwołanie klucza publicznego serwera wymaga metody sprawdzania stanu klucza publicznego serwera. Ta metoda prawdopodobnie użyje klucza publicznego serwera jako dodatkowej kotwicy zaufania lub będzie polegać na mechanizmie listy CRL.

* Musi istnieć niemożliwy do wygaszenia mechanizm, aby urząd certyfikacji dostarczał zaufanemu serwerowi informacje o odwołaniu; oznacza to, że urząd certyfikacji powinien wiedzieć, czy informacje o odwołaniu dotarły do zaufanego serwera, czy nie. Chociaż sam urząd certyfikacji może działać jako zaufany serwer, nie jest to zalecane ze względów bezpieczeństwa; ponadto nie chcemy narzucać architekturze CA wymagań dotyczących wysokiej wydajności. Zaufany serwer musi być systemem o wysokiej wydajności.

* W obszarze CA nie ma standardów zapewniających nieusuwalne mechanizmy przesyłania informacji o odwołaniu do zaufanego serwera. Mechanizmy te mogą być pożądane w jednej z czterech sytuacji:

1. Potrzebujesz najcieńszego klienta PKI

2. Konieczność generowania przychodów z usług CA

3. Musisz sprawdzić zmieniające się dane uwierzytelniające, takie jak dostępny kredyt

4. Konieczność aktualizacji poświadczeń dynamicznych, takich jak pozostały limit kredytowy

Dwie ostatnie sytuacje umożliwiają zaufanemu serwerowi dostarczenie informacji o odwołaniu oraz sprawdzenie lub zmianę poświadczeń subskrybenta. Delta CRL i protokoły odwołania/uwierzytelniania oparte na serwerze, takie jak OCSP (RFC 2560), są zgodne ze standardami i mogą dostarczać te same informacje, co na liście CRL dla pojedynczego certyfikatu przy znacznie mniejszej przepustowości. Wymagają one pewnej formy akceptowalnego uwierzytelniania, ponieważ oryginalny urząd certyfikacji nie będzie dostępny do podpisania.

Podsumowanie zaleceń dotyczących powiadomienia o unieważnieniu

Najbardziej skalowalny i wszechstronny mechanizm powiadamiania o odwołaniu można osiągnąć, stosując kombinację:

* Listy CRL.

* Replikacja wpisu katalogu CA w lokalizacjach określonych przez topologię sieci przedsiębiorstwa w celu szybkiego dostępu do listy CRL.

* Korzystanie z ARL.

* Konsolidacja list ARL dla wszystkich urzędów certyfikacji w domenie za pomocą punktów dystrybucji. Konsolidację uzyskuje się poprzez umieszczenie nazwy urzędu certyfikacji, który może odwołać certyfikat, w rozszerzeniu Punkt dystrybucji listy CRL certyfikatu.

* Konsolidacja wszystkich kodów przyczyn złamania klucza dla wszystkich certyfikatów w domenie za pomocą rozszerzenia Distribution Point. Ta lista CRL może być wystawiana bardzo często, aby spełnić wymagania dotyczące świeżości domeny. Ten mechanizm sprawia, że mechanizm listy CRL jest tak samo aktualny jak OCSP.

* Partycjonowanie informacji o rutynowym odwołaniu przy użyciu list CRL punktu dystrybucji, jeśli listy CRL staną się zbyt duże.

Kilka innych technik może pomóc w poprawie wydajności pobierania list CRL:

* Repozytoria mogą przechowywać zarówno zaszyfrowane listy CRL w celu wysłania do stron ufających, jak i odszyfrowane listy CRL (tekst jawny) w celu wykonywania szybkich wyszukiwań. Przechowywanie obu formularzy zmniejsza obciążenie, które wynikałoby z używania szyfrowania lub deszyfrowania w momencie każdego żądania.

* Jeśli repozytorium nie przechowuje żadnych prywatnych informacji, operacje wiązania do pobierania można skonfigurować tak, aby nie wymagały uwierzytelniania, eliminując w ten sposób kolejne potencjalne wąskie gardło wydajności.

* Rozmiar listy CRL można zmniejszyć, stosując krótki okres ważności certyfikatów, używając zgrubnej nazwy domeny, aby reorganizacja nie unieważniała nazwy, oraz zezwalając na pewne zmiany (np. zmianę nazwy lub przeniesienie) bez wymuszania odwołania.

REGULACJA

Certyfikaty klucza publicznego dla subskrybentów mają określoną ważność .Kropka. Po upływie okresu ważności subskrybenci wymagają nowych certyfikatów klucza publicznego. Istnieją dwa główne powody, dla których certyfikaty klucza publicznego mają ograniczoną żywotność. Jedna dotyczy życia klucza prywatnego w oparciu o potencjalne zagrożenie kryptoanalizą. Innym powodem jest pomoc w kontrolowaniu rozmiaru listy CRL, ponieważ żaden certyfikat nie jest usuwany z listy CRL, dopóki nie wygaśnie. Żaden klucz publiczny nie powinien być używany dłużej niż szacowany czas kryptoanalizy metodą brute-force przy użyciu obecnej technologii (okres zagrożenia kryptoanalizą). W tym momencie do certyfikatu powinien zostać przypisany nowy klucz publiczny (tzn. należy go ponownie kluczować). Jednak przed wygaśnięciem okresu zagrożenia kryptoanalizą ten sam klucz może zostać odnowiony lub ponownie certyfikowany. Certyfikaty można łatwo odnawiać, wysyłając subskrybentom cyfrowo podpisane żądanie do urzędu certyfikacji lub wykonując automatyczne odnowienie przez urząd certyfikacji. W trakcie odnawiania wszelkie informacje (inne niż klucz publiczny subskrybenta) mogą ulec zmianie. W dającej się przewidzieć przyszłości żywotność 1024-bitowego klucza RSA może wynosić 25 lat. Ponowne używanie tego samego klucza z nowymi certyfikatami tak długo, jak to możliwe, zmniejsza liczbę przeszłych kluczy, które należy zdeponować w celu odzyskania lub zweryfikowania starszych plików. Podczas ponownego wprowadzania klucza należy również wziąć pod uwagę poziom zaufania, ale można oczekiwać, że klucze przechowywane w sprzęcie odpornym na manipulacje osiągną pełny okres życia.

Uwaga: NIST SP800-78-3 zaleca, aby po 2013 roku używać tylko kluczy 2048-bitowych. Elementy korzystające z klawiszy programowych są z natury zagrożone określonym atakiem i powinny być używane tylko w przypadku niższych poziomów zaufania.

Certyfikaty można również łatwo zmienić, wysyłając subskrybentowi podpisaną cyfrowo wiadomość z żądaniem ponownego wprowadzenia klucza, która zawiera również nowy klucz publiczny. Wiadomość jest podpisana przy użyciu bieżącego klucza prywatnego, dzięki czemu można ją zweryfikować przy użyciu bieżącego klucza publicznego. Jeśli subskrybent, którego klucz jest ponownie kluczowany, jest CA, w grę wchodzą również te wymagania:

* Strony ufające powinny mieć możliwość weryfikacji łańcuchów certyfikatów po ponownym kluczowaniu urzędu certyfikacji.

* Strony ufające powinny mieć możliwość weryfikacji list CRL wystawionych przez urząd certyfikacji.

* Ponowne kluczowanie nie powinno mieć wpływu na PKI. Tylko dlatego, że jeden urząd certyfikacji ponownie klucze, inne urzędy certyfikacji lub jednostki końcowe nie powinny mieć ponownego klucza.

* Długość ścieżek certyfikatów powinna być zminimalizowana.

* Wpływ operacyjny na podmioty PKI powinien być minimalny.

Dobrym sposobem na spełnienie tych wymagań jest:

* Wydaj wszystkie aktualne ważne certyfikaty podczas ponownego klucza, bez zmiany okresów ważności w certyfikatach subskrybenta.

* Kontynuuj podpisywanie list CRL wszystkimi aktualnymi ważnymi kluczami prywatnymi. Spowoduje to powstanie wielu list CRL z tymi samymi informacjami. Klucz prywatny CA jest uważany za ważny do momentu wygaśnięcia wszystkich certyfikatów podpisanych przy użyciu tego klucza.

Jeśli urząd certyfikacji jest kotwicą zaufania, może użyć jednego z dwóch podejść do ponownego wprowadzenia klucza w paśmie, w niezaufanej sieci:

1. Urząd certyfikacji może wysłać wiadomość o ponownym kluczu, która zawiera nowy klucz publiczny i jest podpisana przy użyciu bieżącego klucza. Urząd certyfikacji musi upewnić się, że wszyscy subskrybenci otrzymali i przetworzyli komunikat o ponownym kluczu przed wygaśnięciem bieżącego klucza.

2. CA może dostarczyć skrót następnego klucza publicznego i parametrów (jeśli algorytm kryptograficzny ma parametry; RSA nie ma parametrów, ale Digital Signature Standard [DSS] ma) z bieżącym kluczem. Gdy nadejdzie czas opublikowania nowego klucza publicznego, urząd certyfikacji może opublikować nowy certyfikat klucza publicznego z podpisem własnym, który zawiera nowy klucz publiczny i parametry, a także skrót następnego klucza publicznego i parametrów.

ODZYSKIWANIE KLUCZY

Klucze publiczne subskrybenta mogą służyć do szyfrowania kluczy szyfrowania danych (w przypadku szyfrowania kluczem symetrycznym). Takie klucze szyfrowania danych są używane do szybkiego szyfrowania danych przy niższym nakładzie szyfrowania z kluczem symetrycznym. Subskrybenci wymagają swoich kluczy prywatnych do odszyfrowania kluczy szyfrowania danych, a tym samym umożliwienia odszyfrowania danych. Niezwykle ważne jest rozróżnienie między kluczami podpisywania a kluczami szyfrowania danych. Ten pierwszy (każdy klucz, który zapewnia niezaprzeczalność) może nigdy nie zostać poddany odzyskiwaniu klucza; te ostatnie mogą być

chronione za pomocą technik odzyskiwania kluczy. Klucze zaufania o wysokim poziomie mogą wymagać oddzielnego klucza identyfikacyjnego, którego nie można użyć do podpisania dokumentu; ten klucz logowania powinien mieć tylko bit podpisu, a nie bit niezaprzeczalności ustawiony w rozszerzeniu Użycie klucza. Czasami token klucza prywatnego subskrybenta (np. dyskietka, dysk twardy, karta inteligentna itp.) może zostać uszkodzony lub subskrybent może zapomnieć hasło powiązane z tokenem. Podobnie, czasami subskrybent może być niedostępny, ale pracodawca subskrybenta może być zmuszony do odszyfrowania informacji firmowych zaszyfrowanych przez zaginionego subskrybenta. Techniki odzyskiwania kluczy zostały zaprojektowane w celu zaspokojenia tych nagłych potrzeb w zakresie dostępu do zaszyfrowanych informacji. Z natury są one formą tylnych drzwi do kluczy, ale nakładają również dodatkowe koszty ogólne. W związku z tym potrzebę zapewnienia odzyskiwania klucza należy starannie wyważyć w stosunku do potencjalnych kosztów i złożoności. Dwie najpopularniejsze formy mechanizmów odzyskiwania klucza to:

1. Klucz depozytowy. W ramach tego formularza długoterminowy prywatny klucz odszyfrowywania subskrybenta jest dostarczany zaufanej stronie trzeciej zwanej agentem odzyskiwania klucza (KRA).

2. Kluczowa enkapsulacja. W ramach tego formularza subskrybent szyfruje klucz szyfrujący dane przy użyciu klucza publicznego KRA, aby KRA mogła odszyfrować dane.

Z tych dwóch schematów klucz depozytowy staje się coraz szerzej dostępny w produktach PKI, ponieważ jest łatwiejszy do wdrożenia na poziomie infrastruktury. Jest również niezależny od granic organizacyjnych między nadawcą a odbiorcą zaszyfrowanej komunikacji. Jeśli prywatny klucz szyfrowania daty strony jest zdeponowany, wówczas komunikacja z tą stroną może zostać odszyfrowana. Subskrybenci mogą zawsze odzyskać swój własny klucz szyfrowania danych z systemu odzyskiwania kluczy. Uprawnione osoby trzecie, takie jak pracodawca subskrybenta, również mogą zażądać kluczy. Taka upoważniona strona nazywana jest żądaniem odzyskania klucza (KRR). Wszystkie składniki podlegają zasadom odzyskiwania kluczy (KRP) i powiązanym oświadczeniom dotyczącym praktyk odzyskiwania kluczy (KRPS). KRP i KRPS są zbliżone do Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, ale mają pewne różnice. Jedna z głównych różnic dotyczy sekcji technicznych zabezpieczeń. Istnieje kilka wymagań dotyczących sprawdzania protokołów komunikacyjnych między składnikami w celu zapewnienia poufności, integralności i autoryzacji. Rysunek 37.13 ilustruje elementy systemu odzyskiwania klucza, jak zostałoby to wyrażone w KPRS. Ogólna krytyka odzyskiwania kluczy polega na tym, że zapewnia tajemnice jednej stronie, a mianowicie KRA. Jednym ze sposobów złagodzenia tych obaw jest udostępnienie sekretu wielu odbiorcom w sposób, który wymaga współpracy (jeśli jest autoryzowana) lub zmowy (jeśli nie jest) pomiędzy dwoma lub więcej posiadaczami zdeponowanej tajemnicy. Na przykład superszyfrowanie (szyfrowanie tekstu zaszyfrowanego) może utrudnić nieautoryzowane odkrycie klucza.

Tajny klucz S jest szyfrowany kluczem publicznym jednego odbiorcy (powiedzmy K1), tworząc tekst zaszyfrowany, reprezentowany jako E(S, K1), a następnie ten zaszyfrowany tekst jest superszyfrowany przy użyciu klucza publicznego drugiego odbiorcy, K2, w celu utworzenia szyfrogram E(E(S, K1), K2). W przeciwieństwie do szyfrowania tej samej wiadomości dla dwóch odbiorców, gdzie każdy odbiorca może odszyfrować tekst zaszyfrowany niezależnie, superszyfrowanie wymaga odszyfrowania przez każdego odbiorcę w odwrotnej kolejności priorytetu. Tak więc, jeśli użytkownik szyfruje tajny klucz za pomocą klucza publicznego A, a następnie superszyfruje zaszyfrowany tekst za pomocą klucza publicznego B, odzyskanie klucza wymaga odszyfrowania przez użycie odpowiedniego klucza prywatnego, a następnie odszyfrowania wynikowego zaszyfrowanego tekstu przez A za pomocą klucza prywatnego tego użytkownika. Aby użyć superszyfrowania, aby mniej niż wszyscy odbiorcy mogli odszyfrować klucz, nadawca szyfruje do pierwszej grupy odbiorców, a następnie superszyfruje do drugiej grupy odbiorców. W ten sposób każdy z członków pierwszej grupy i każdy członek drugiej grupy

odbiorców może współpracować w celu odszyfrowania tajnego klucza. Ta technika umożliwia depozyt klucza nawet w przypadku braku formalnej infrastruktury PKI, na przykład w nieformalnych sieciach zaufania przy użyciu PGP. Innym rozwiązaniem utrudniającym zmowę w depozycie kluczy jest podzielenie klucza przy użyciu reguły n out of m Shamira12. do odtworzenia tajnego klucza. Tak więc n–1 lub mniej osób będących w zmowie nie może określić nawet jednego bitu zdeponowanego klucza. Udana zmowa wymaga co najmniej n osób. Podejście oparte na kluczu dzielonym można zastosować do depozytu klucza, w którym to przypadku klucz prywatny można podzielić i różne podziały można udostępnić różnym agentom KRA. Alternatywnie, podejście podzielonego klucza można zastosować do enkapsulacji, gdzie klucz sesji może być podzielony, a różne podziały mogą być szyfrowane przy użyciu kluczy publicznych różnych KRA.

Ta strategia teoretycznie pozwala również na wykonanie pełnej rekonstrukcji tajnego klucza przez autoryzowanego odbiorcę kluczy częściowych, zamiast przez dowolnego agenta depozytowego.

ZARZĄDZANIE PRZYWILEJAMI

Podstawowym celem PKI jest zapewnienie uwierzytelniania jednostek w globalnym, rozproszonym środowisku. W większości systemów i aplikacji

uwierzytelnianie staje się podstawą kontroli dostępu. Istnieją trzy podstawowe sposoby wdrożenia kontroli dostępu:

1. Systemy i aplikacje mogą samodzielnie wykonywać kontrolę dostępu. PKI nadal zapewnia ramy uwierzytelniania.

2. Uprawnienia, atrybuty, role, prawa i autoryzacje mogą być przenoszone w certyfikacie klucza publicznego w rozszerzeniu atrybutu katalogu podmiotu.

3. Uprawnienia, atrybuty, role, prawa i autoryzacje mogą być przenoszone w certyfikacie atrybutu. Standard X.509 jest aktualizowany w celu uwzględnienia koncepcji certyfikatów atrybutów. Certyfikaty atrybutów zawierają uprawnienia i autoryzacje zamiast klucza publicznego, dzięki czemu zapewniają rozproszoną strukturę autoryzacji. Certyfikaty logowania, podpisywania i szyfrowania użytkownika nigdy nie powinny być używane do przenoszenia autoryzacji lub informacji o aplikacji. W razie potrzeby dla tych zadań można wydać oddzielne certyfikaty. Takie certyfikaty autoryzacyjne mogą być wydawane codziennie, a nawet na krótsze okresy, eliminując potrzebę posiadania listy CRL, ponieważ certyfikat wygasłby, zanim zostałby wydany. Te certyfikaty autoryzacyjne mogą być używane zamiast Kerberos (grecki mitologiczny trójgłowy pies, który strzeże wejścia do Hadesu). Rysunek 37.14 podsumowuje zalety i wady każdego z trzech podejść. Czynniki te należy wziąć pod uwagę przy projektowaniu infrastruktury dostępowej. Chociaż certyfikat atrybutów wydaje się być najnowszą modą w świecie PKI, użytkownicy powinni uważnie przestudiować umieszczanie uprawnień w certyfikatach kluczy publicznych, aby zaoszczędzić na kosztach wdrożenia infrastruktury zarządzania uprawnieniami (PMI) w porównaniu z kosztami PKI.

ZAUFANE USŁUGI ARCHIWALNE I ZAUFANE ZNACZNIKI CZASU

Technologia PKI wspiera globalny handel elektroniczny dzięki wykorzystaniu technologii podpisu cyfrowego. Technologia podpisu cyfrowego to mechanizm wykrywania lub pasywny. Innymi słowy, technologia nie uniemożliwia komuś modyfikowania danych przechowywanych lub przesyłanych ani podszywania się pod kogoś innego. Technologia wykrywa jedynie, że podjęto próbę zmodyfikowania danych lub że ktoś próbował podszyć się pod kogoś innego. W sądzie można zakwestionować podpisy cyfrowe długo po ich zastosowaniu, jeśli na przykład upłynął okres zagrożenia kryptoanalizą kluczy. W takich okolicznościach przedstawienie dokumentu ze zweryfikowanym podpisem cyfrowym może nie

przeszkodzić w odrzuceniu. Strona może twierdzić, że minął okres zagrożenia kryptoanalizą, a klucz prywatny mógł zostać odkryty lub złamany przez przeciwnika. Aby złagodzić oba te zagrożenia — uszkodzenie danych i wygaśnięcie okresu zagrożenia kryptoanalizą — wymagane są zaufane usługi archiwalne dla transakcji, które mogą prowadzić do tego rodzaju sporu. Taka usługa archiwalna byłaby również w stanie zabezpieczyć powiązane certyfikaty i listy CRL. Zaufane usługi archiwizacji powinny zależeć od mechanizmów kontrolnych, takich jak zabezpieczenia fizyczne, stabilne nośniki (np. urządzenia jednokrotnego zapisu, odczytu-wielu [WORM]) oraz odpowiednie techniki zachowania czytelności pomimo zmieniających się technologii. Takie usługi powinny umożliwiać bezbłędną transkrypcję danych na starszych nośnikach oraz tłumaczenie przestarzałego kodowania na bardziej nowoczesne nośniki oraz na obecne schematy kodowania. Na przykład dane zakodowane w formacie Extended Binary Coded Decimal Interchange Code (EBCDIC) na dziewięciościeżkowych taśmach magnetycznych mogą być kopiowane na dyski optyczne przy użyciu kodowania ASCII. Powiązana technologia to zaufany znacznik czasu, w którym zaufana strona trzecia dołącza aktualny ważny czas do dokumentu i podpisuje go, aby udowodnić istnienie dokumentu w określonym czasie. Jeśli właściciel dokumentu nie chce ujawniać zawartości dokumentu serwerowi znacznika czasu, zamiast tego może zostać ostemplowany i podpisany skrót dokumentu. W większości aplikacji zaufana usługa archiwizacji może wyeliminować potrzebę korzystania z usługi zaufanego znacznika czasu, ponieważ na dłuższą metę zaufana usługa archiwizacji może poświadczyć czas transakcji. W krótkim okresie obie strony mogą datować i cyfrowo podpisywać transakcję po jej sfinalizowaniu, dzięki czemu jest ważna jako umowa. Jeśli data jest nie do zaakceptowania dla którejkolwiek ze stron – jest albo zbyt odległa w przyszłości, albo w przeszłości – strona ta może albo odrzucić transakcję, albo natychmiast wszcząć procedurę rozstrzygania sporu.

KOSZT INFRASTRUKTURY KLUCZU PUBLICZNEGO

Jednym z błędnych przekonań na temat technologii infrastruktury klucza publicznego jest to, że jest ona zbyt kosztowna, ale koszty te należy porównać z alternatywami. Poza podjęciem poważnego ryzyka nie ma innej praktycznej technologii niż kryptografia do ochrony danych przesyłanych przez niezaufaną sieć. Jedynym wyborem jest zatem między kryptografią klucza symetrycznego a kryptografią klucza publicznego. Oprócz trudności związanych z dystrybucją i obsługą symetrycznych, tajnych kluczy, takie kryptosystemy wymagają około n2 kluczy dla grupy n osób, które muszą się ze sobą komunikować. Kryptosystem tajnego klucza wymaga, aby n2 kluczy było utrzymywanych w tajemnicy, z zachowaniem ich integralności; PKI wymaga zarządzania tylko n kluczami. Oczywiście utrzymanie integralności n kluczy powinno być tańsze niż zarządzanie n2 kluczami oraz ich poufnością i integralnością. PKI jest potrzebne do zarządzania kluczami publicznymi. Koszty PKI wydają się duże, gdy muszą zapewniać globalne zaufanie i interoperacyjność, czego nie wymaga się od większości systemów lub infrastruktur. Obecnie żadna inna technologia nie działa tak dobrze ani nie jest tak opłacalna jak PKI, umożliwiając globalną, bezpieczną, zaufaną komunikację i handel elektroniczny. Alternatywą jest podjęcie ryzyka bez PKI lub kontynuowanie podejścia opartego na papierach zaufania z ubiegłego wieku.