

Mobiltelefonen blir säkerhetskanal genom trådlös PKI

av Sverker Arvidson [sverker.arvidson@bankid.com]

Lärdomar från WAP-tiden

WAP står för WirelessApplicationProtocol och är ett protokoll som möjliggör för dig att ”surfa” med din mobil. Enbart specifika WAP-sidor kan nås och adressen är vanligtvis wap.xx.xx, ex. wap.campuzmobile.com.

År 1999 gick en ”WAP-hype” över Europa och USA. Tydligast var trenden i de Nordiska länderna. Sverige och Finland var vid den tiden mobilutvecklingens centrum genom företagen Ericsson och Nokia. WAP skulle möjliggöra Internet även för mobiltelefoner. Förhoppningarna var enorma. Planer växte fram för att utveckla mobila applikationer.

Det räckte att små nystartade företag hade WAP och Internet på sina program för att aktiekurserna skulle skjuta i höjden. Även en del banker greps av yran och bestämde sig för att utveckla bankapplikationer för mobiler. Flera banker lanserade också WAP-tjänster.

De mobila bankapplikationerna blev aldrig någon succé. Trots intensiv marknadsföring anslöt sig endast några tusentals kunder till de mobila tjänsterna. Det finns flera samverkande förklaringar:

- Mobiltelefonerna (terminalerna) var omogna och instabila. Skärmfönstren var små, vilket medförde att presentationen inte blev tydlig och pedagogisk.
- Det var mycket svårt att parametersätta mobilerna. Parametersättningen var då en manuell process där ett antal värden skulle matas in i den mobila enheten för att den skulle kunna fungera som en WAP-terminal. Instruktionerna hur man skulle göra var skrivna av tekniker och i princip omöjliga att förstå för gemene man. Redan i detta moment gav många presumtiva kunder upp. I dag överförs nödvändiga parametrar med hjälp av SMS och parametersättningen är inte längre ett problem.
- GPRS (teknik för mobil datakommunikation med högre hastighet) var ännu inte införd vid denna tid. Man var alltså hänvisad till att använda normal GSM-kommunikation. Bildväxlingarna för mobilkunden blev mycket långsamma. Dessutom tickade taxepulserna även under den tid då slutkunden bara tittade på innehållet, t ex sina transaktioner. Detta fick abonnenten betala och det var inte helt billigt för en privatperson.
- WAP-standarden (1999) innehöll ingen säkerhetsmetod. Detta medförde att innehållet i de mobila banktjänsterna blev starkt begränsade. Bankerna kunde inte med tillräcklig

säkerhet avgöra vem kunden var. Det var naturligtvis tekniskt möjligt att använda engångskoder med hjälp av dosa eller ”skraplott”. Rent praktiskt var det dock orimligt att tänka sig att kunden utförde sina transaktioner med mobilen i ena handen och dosan i den andra. En lösning var att införa en ”fixed” pin-kod, som gav en betydligt lägre säkerhetsnivå. De nödvändiga begränsningarna gjorde att kunden t.ex. bara kunde göra överföringar mellan egna konton. Man kunde få minutaktuella börskurser men handel med aktier var för riskfyllt.

Summan av ovanstående brister förklarar varför införandet av mobila banktjänster år 1999 inte blev en lyckad satsning. Begreppet WAP blev, i vissa kretsar, närmast jämförbart med en svordom.

Nya, säkra tag

Tanken med att utnyttja mobilen i Internetsammanhang var dock fortfarande lockande. En bit in i år 2000 möttes personer från Nokia, TeliaSonera och Handelsbanken vid ett flertal tillfällen för att diskutera möjliga utvecklingsvägar.

Diskussionerna handlade inledningsvis om det var möjligt att tillföra Handelsbankens befintliga mobila banktjänst en mer avancerad säkerhet. Standardiseringen av WAP hade fortsatt och nu fanns specificerat hur en säkerhetslösning byggd på PKI skulle utformas (Wireless PKI eller WPKI). Eftersom Handelsbankens Internettjänst (Internetbank) redan använde PKI som säkerhetsmetod skulle en WPKI-baserad mobiltjänst lättare kunna integreras. De begränsningar som fanns i tjänsteutbudet i den dåvarande mobila lösningen skulle helt kunna elimineras med en säkerhetsteknik som WPKI. Mobila tjänstelösningar byggda på WAP hade emellertid fått ett så dåligt rykte att vi bedömde möjligheten att få vidareutveckla Handelsbankens mobila tjänst som utsiktslös. Istället växte idén fram att ge mobiltelefonen egenskaper, som medförde att den kunde bli en säkerhetsenhet (trusted device) för användning över Internet. Den säkerhetsteknik som skulle användas var just WPKI. Det kritiska i en PKI-lösning är hur väl den privata nyckeln skyddas. I vårt tänkta fall skulle den privata nyckeln lagras i mobilens SIM-kort och aldrig lämna denna krets. Lösningen blir därmed jämställd med sådana som använder sig av smarta kort, s.k. hårda lösningar. Med en sådan teknik inbyggd i mobilen skulle man både kunna identifiera sig över Internet och signera transaktioner. I jämförelse med t.ex. säkerhetslösningar som bygger på dosor för generering av engångskoder har mobiltelefonen ett antal fördelar:

- Nästan varje vuxen svensk har en mobiltelefon. Mobilen kan betraktas som en personlig utrustning.
- Man bär oftast mobilen med sig. Skälet är att man med röstsamtal vill bli nådd eller nå andra. Om mobilen också skulle innehålla en säkerhetsfunktion finns även denna funktion tillgänglig när man behöver den. En säkerhetsdosa för engångskoder är förmodligen kvar hemma om man oförutsett behöver genomföra en transaktion från en annan plats.
- Med mobilen uppnår man full PKI-funktionalitet, d.v.s. både identifiering och signering.

I diskussionen mellan de tre parterna skisserades följande scenario:

”Du är kund i en Internetbank som använder WPKI som säkerhetsmetod. När du, från din PC, kopplar upp dig till Internetbanken, i syfte att logga in, möts du av en ny inloggningsmöjlighet – logga in mobilt. Du klickar på detta alternativ och någon sekund senare får du en signal i din mobiltelefon. I mobilens display uppmanas du att avge ditt lösenord (WPKI-lösenordet som du själv tidigare har valt). När du gör detta utöses den kryptologiska bearbetningen med hjälp av den privata nyckeln. Den centrala Internetbanksapplikationen kan nu avgöra att du är du. På din PC öppnas nu de tjänster som du kan göra som inloggad. Du gör nu, på din PC, en överföring av pengar från ett konto till ett annat. Därefter klickar du på Signering(Underteckna). Nu upprepas föregående procedur. Mobilen avger en signal och i displayen ser du den överföringstransaktion som du nyss registrerade på din PC. Du uppmanas på nytt att avge ditt lösenord och därmed undertecknas/signeras din transaktion.”

Detta scenario konstaterades vara så intressant att ett praktiskt prov (proof of concept) genomfördes. TeliaSonera lät tillverka ett SIM-kort som innehöll en privat nyckel. En simulerad Internetbank byggdes. Med hjälp av en standard PC och en mobil med ett PKI-baserat SIM-kort genomfördes lyckade tester enligt scenariot ovan. Den simulerade Internetbanken hanterade två olika kanaler synkront, en säkerhetskanal mot mobilen och en informationskanal över Internet mot PC'n.

En viktig slutsats i WPKI-sammanhang är att mobilkanalen alltid är en säkerhetskanal. Informationskanalen kan rikta sig mot en PC, men även en digital-TV eller mobilen själv kan vara målenhet. I praktiken innebär detta att om man vill ha en stor informationsyta (t.ex. en deklaraionsblankett) så använder man en PC i kombination med mobilen. Om man gör en enkel överföring av pengar mellan två konton kan både säkerhet och själva transaktionen genomföras från samma mobil. Den i inledningen beskrivna säkerhetsbristen för mobila applikationer är nu löst om WPKI genomförs.

Säkerhet är en samhällelig infrastrukturfråga

En annan viktig slutsats parterna drog är att WPKI är en infrastruktursatsning. Banken kan inte acceptera att bara kunder med TeliaSonera-abonnemang eller kunder med Nokiatelefoner får tillgång till den nya funktionaliteten. Omvänt kunde inte operatören eller mobiltillverkaren utveckla denna infrastruktur för en enda bank.

Eftersom bankerna redan har genomfört en gemensam säkerhetsutveckling som resulterat i BankID (e-legitimation) var det naturligt att placera en kommande utveckling i det bankgemensamma bolag som redan fanns. BankID konceptet skulle därmed kompletteras med ytterligare en säkerhetsmetod. Nu gällde det att få med ytterligare operatörer och telekomindustri i infrastruktur bygget. Intresset från dessa parter var så stort att man kunde besluta om ett gemensamt projekt.

Det gemensamma projektet startade i februari 2004. Målet var att ta fram specifikationer för hur en WPKI-infrastruktur ska byggas. Bl.a. skulle gränssnitten mellan mobiloperatörens system och en CA (certificate authority, e-legsutgivare) specificeras liksom konstruktionen för de nya SIM-korten. Dessutom skulle en demonstrator konstrueras som i verkligheten använde alla ingående

funktioner. I projektet ingick representanter från TeliaSonera Sverige, Telenor Sverige, Tele2, Ericsson, bankerna bakom BankID och deras bankgemensamma bolag. Projektet avslutades i december 2004. En komplett samling specifikationer och en fullt ut fungerande demonstrator finns nu som resultat av projektarbetet.

Välkomna ta del av specifikationerna

Parterna kände det viktigt att publicera specifikationerna. Dels för att de förhoppningsvis kan utgöra ett underlag för standardisering, dels för att undvika att någon tar patent på hela eller delar av det gemensamma projektresultatet. I mars 2005 publicerades därför specifikationerna, tillsammans med en del övrigt material, på hemsidan www.wpki.net. För att förvalta och vidareutveckla specifikationerna bildade parterna dessutom en förening: ”WPKI-föreningen”. Ytterligare ett syfte med föreningen är sprida kunskap om konceptet och verka för kommande standardiseringar. Avsikten är att ta in nya medlemmar utöver de företag som grundade föreningen. Vi hoppas på medlemmar från både myndigheter och privata företag.

Det unika i det genomförda projektarbetet är inte bara resultatet i form av specifikationer och demonstrator utan också att det skett i samarbete mellan banker och operatörer. Något som skulle ha varit omöjligt för sex, sju år sedan.

De parter som så önskar är nu fria att utveckla WPKI inom sina egna koncept. Avsikten är dock att man i grunden använder de gemensamma specifikationerna. Inom ramen för BankID pågår nu utredningar för att undersöka hur WPKI ska implementeras i detta koncept. En avgörande faktor är också att rimliga ekonomiska villkor kan uppnås mellan operatörerna och bankerna.