MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Bilaga 1-Teknisk beskrivning av de föreslagna funktionerna

Egenskapskrav och förutsättningar

Följande tekniska egenskapskrav har beaktats vid utformningen av det föreslagna systemet:

1. Beträffande bäraren ska tillgänglig och standardiserad teknik användas för att möjliggöra en hög grad av kostnadseffektivitet och kort införandetid.
2. För att uppfylla kraven för den högsta tillitsnivån ska innehavarens nyckelmaterial skyddas genom hårdvara som bör kunna vara certifierad enligt relevant internationellt vedertagen norm.
3. Verifieringen av användarens identitet bör i användningsfasen inbegripa kontroller mot centralt placerade systemkomponenter, främst i syfte att
    a. avlasta det säkerhetsmässiga beroendet till den tekniska bäraren
    b. kunna spärra e-legitimationen centralt efter ett visst antal felaktiga försök att ange den personliga koden där också en tidsfaktor ingår
    c. kunna ge underlag för att framställa en sammanvägd riskindikator baserad på vissa parametrar i användningsmönster som kan användas av förlitande aktör för att avgöra om vidare kontroller behöver genomföras för att förhindra obehörig användning av den statliga e-legitimationen.
4. Erbjuda en hög teknisk säkerhet utifrån tillgänglig teknik och robusta säkerhetsfunktioner, samt en hög grad av flexibilitet för att kunna ansluta såväl offentliga som privata leverantörer av identitetsintyg. Det föreslås därför att
    a. all kommunikation mellan användare och integrationslager ska ha ett robust kryptografiskt skydd mot insyn och förändring i mer än ett skikt
    b. alla anrop från användare till integrationslager ska vara kryptografiskt signerade med det aktiva kortets kortautentiseringsnyckel (som således används utan personlig kod)
    c. användarens personliga kod aldrig får exponeras för vare sig infrastrukturkomponenter (t.ex. proxy-funktioner) eller integrationslager

   d. ingen del av den tekniska säkerheten ska bero på att klientprogramvarans utformning hålls dold. Klientprogramvarans integritet kommer dock oundvikligen vara av säkerhetsmässig betydelse för interaktionen mot användaren, så att den information användaren får genom dialoger m.m. är korrekta och beskriver de verkliga skeendena.

5. Vid misslyckade försök att ange personlig kod bör systemet på ett kontrollerat sätta ha förmåga att begränsa ytterligare försök i flera steg genom successivt ökade tidsintervall, för att slutligen på automatisk väg kunna spärra e-legitimationen permanent.

Grundkomponenter

För att minimera utvecklingsarbetet föreslås att en standardiserad teknik för det aktiva kortet används, PIV[1] (*Personal Identity Verification*). Detta är den egentligen enda förkommande fullständiga specifikationen för denna typ av kort som uppfyller funktionskraven. Andra typer bygger vanligtvis i varierande grad på den internationella standarden ISO/IEC 7816-15[2]. Denna standard är dock endast ett ramverk, inom vilket variationsmöjligheterna är närmast obegränsade. E-legitimationer med denna standard som utgångspunkt fungerar således på vitt skilda sätt, som ofta är leverantörsspecifika. Att välja kort som bygger på detta ramverk driver utvecklingskostnader, skapar leverantörsinlåsningar och minskar den tekniska interoperabiliteten, jämfört med en striktare specifikation som i tillräcklig detalj preciserar hur kortet ska fungera.

Att basera den statliga e-legitimationen på PIV-standarden får även till följd att ett flertal leverantörer utan särskilda anpassningar kan tillhandahålla kompletta certifierade och likvärdiga produkter på den öppna marknaden, med de erforderliga funktioner som skulle krävas. Det finns även ett stort utbud av programbibliotek och standardapplikationer att tillgå som bygger på öppen källkod.

Följande underspecifikationer är relevanta i sammanhanget:

- SP 800-78-4: Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- SP 800-73-4: Interfaces for Personal Identity Verification

[1] https://csrc.nist.gov/Projects/PIV/PIV-Standards-and-Supporting-Documentation

[2] ISO/IEC 7816-15:2016 – *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

Kortens primära nyckelmaterial föreslås baseras på elliptiska kurvor[3] med parametrar enligt NIST P-256[4]. Krav bör ställas på att också stödja RSA[5] med en moduluslängd om minst 2048 bitar som alternativ algoritm, om sådan skulle komma att krävas i något skede av säkerhets- eller interoperabilitetsskäl.

Kortleverantörens roll

Det antas att leverantör av kort behöver upphandlas av Digg. Dennes roll som kortproducent blir att ordna så att rätt typ av chip lamineras i den typ av plast som kravställts, kvalitetskontrollera chippet och lamineringen, påföra tryck och löpnummer, ladda kortapplikationen (PIV), skapa nycklar på kortet (i kortets egna omgivning) för kortautentisering (*card authentication*) och säker kortkommunikation (*secure messaging*) samt ordna med självsignerade certifikat för dessa tillämpningar.

Det är värt att notera att det även krävs att utfärdarcertifikat tillhörande Digg lagras i kortet för att i ett senare skede kunna upprätta en säker kommunikation mellan Diggs system och kortet. Uppgifter om kortets löpnummer samt de publika nycklarna överförs till Digg och registreras i registret över innehavare. De producerade korten packas i lådor och förseglas med säkerhetsemballage, för att sedan distribueras till utgivningsställena.

På detta sätt reduceras det säkerhetsmässiga beroendet till leverantören och leverantörsinlåsningar minimeras. Bedömningen är att det inte krävs en fullständig infrastruktur för öppna nycklar (Public Key Infrastructure, PKI) för dessa kortnycklar, utan det är tillräckligt att de infrastrukturkomponenter som Digg tillhandahåller har tillgång till kortens publika nyckelmaterial genom ett register. Att undvika att skapa en separat PKI för dessa funktioner förväntas också leda till minskade kostnader, enklare kortproduktion, minskade leverantörsinlåsningseffekter och kortare införandetid.

Personalisering av kortet med certifikat för elektronisk identifiering och underskrift kan sedan ske på distans, genom funktionen för säker kortkommunikation. Dessa certifikat behöver stämplas av en betrodd certifikatutfärdare inom ramen för en traditionell PKI och föreslås som en påbyggnadsfunktion till lösningen, och endast för de användare som begär funktionen och som därför har behov av dessa certifikat. Detta då riskerna med obehörig användning bedöms öka, eftersom den kontroll som

[3] ISO/IEC 14888-3:2006 – *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*, avsnitt 2.3.
[4] FIPS PUB 186-4 – *Digital Signature Standard (DSS)*, bilaga D, avsnitt D.1.2.3.
[5] RSASSA-PSS eller RSASSA-PKCS#1 v1.5 enligt RFC 3447 – *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*, avsnitt 8.

annars kan göras genom de centrala infrastrukturkomponenterna går om intet. Samtidigt som relativt få användare förväntas ha behov av att genomföra underskrifter och identifieringar oberoende av den statliga identifieringstjänsten som Digg tillhandahåller.

Kommunikationsgränssnitt

Korten föreslås kommunicera med klientprogramvaran primärt via kontaktlös närfältskommunikation (NFC).[6] Huruvida kommunikation även ska vara möjlig via elektriskt gränssnitt kan behöva utredas vidare. Fördelen med ett elektriskt gränssnitt är enklare och därmed billigare läsare för dem som önskar använda korten med vanliga datorer. Nackdelarna är möjligen något sämre hållbarhet.

Via båda gränssnitten kan, som tidigare nämnts, ytterligare personalisering göras. Det är också möjligt att endast tillåta sådan personalisering via ett av gränssnitten. Av robusthetsskäl rekommenderar tillverkare av kort vanligen att personalisering av kort endast sker via elektriskt gränssnitt, då kortet kan bli obrukbart om kommunikationen bryts under personaliseringsprocessen.

Fysisk utformning

Kortet som föreslås är i bankkortstorlek enligt ISO/IEC 7810[7] (id-1) men har ingen personlig prägling. Varje kort har ett förtryckt löpnummer för att underlätta identifiering och koppling till fysisk person, men det är de förgenererade kortnycklarna som unikt identifierar den elektroniska id-handlingen. På baksidan av kortet föreslås en skrivbar yta som innehavaren kan använda för att märka kortet med ett personligt kännetecken.

Personlig kod

Varje användare har en personlig kod kopplat till sitt kort. Koden är enbart känd av användaren; de centrala infrastrukturkomponenterna lagrar endast det underlag för nollkunskapsbevis som behövs för att verifiera den personliga koden. Detta medför att registret över innehavare inte har någon direkt information om användarens personliga kod – varken i klartext eller i form av ett kryptografiskt kondensat. Det betyder också att användarens personliga kod aldrig överförs till den centrala infrastrukturen. Det underlag som krävs genereras från den angivna personliga

[6] Typ A och B enligt ISO/IEC 14443 – *Identification cards – Contactless integrated circuit cards – Proximity cards*, del 1 till 4.
[7] ISO/IEC 7810:2019 – *Identification cards — Physical characteristics*

koden i användarens omgivning (klientprogramvaran, respektive användarens webbläsare då aktivering sker med stöd av sådan).

Risken för att användarnas personliga kod röjs genom intrång eller misstag kan därmed minimeras, samtidigt som de centrala komponenterna förmår att automatiskt agera reaktivt på misslyckade identifieringsförsök.

Undantag från dessa principer utgörs av den aktiveringskod som skapas 24 timmar efter att kortet överlämnades till användaren, om aktivering med pass eller nationellt id-kort inte skett innan dess. Aktiveringskoden görs känd för den process som skapar den samt för den process och utrustning som skriver ut användarens kodkuvert. I övrigt sker hanteringen på samma sätt som för den personliga koden. Aktiveringskoden är således i praktiken användarens första personliga kod fram tills dess att kortet aktiverats.

Verifiering av personlig kod

Vid verifiering av personlig kod används det nollkunskapsbevis som sätts samman med stöd av användarens klientapplikation.

- Användarens personliga kod kontrolleras mot integrationslagret med ett nollkunskapsbevis (*zero-knowledge proof*).
- Val av autentiseringsprotokoll bör utredas vidare i implementionsfasen. En första analys visar att OPAQUE[8] med någon av de rekommenderade standardkonfigurationerna kan vara en lämplig metod, alternativt SRP6a[9] tillsammans med Argon2[10] som nyckelderiveringsfunktion.

Om fel personlig kod anges ett antal gånger reagerar centralsystemet på detta genom att införa en fördröjning till nästa tillåtna försök. Denna fördröjning kan ökas successivt för att bromsa möjligheterna för obehöriga att gissa rätt kod. Efter visst antal felaktiga försök spärras dock e-legitimationen permanent, och innehavaren hänvisas till att skaffa en ny.

Byte av personlig kod

Byte av personlig kod sker på samma sätt som vid verifiering av personlig kod, med skillnaden att underlag för ett nytt nollkunskapsbevis också framställs och överförs

[8] https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque
[9] http://srp.stanford.edu/design.html
[10] RFC 9106 – *Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications.*

genom integrationslagret. Användaren kan byta sin personliga kod via klientapplikationen.

Förlorad personlig kod

Om användaren förlorar (glömmer) sin personliga kod är denne hänvisad till att skaffa en ny e-legitimation, på det sätt som beskrivs i kapitel 5.

Register över innehavare

Samtliga tillverkade kort registreras i ett centralt register. Registret förväntas innehålla följande uppgifter:

- Kortets löpnummer
- Kortets publika nyckelmaterial (för kortautentisering och säker kortkommunikation samt eventuella personliga certifikat)
- Kortets bärartyp (etikett som anger typ av kort, om flera olika typer skulle finns i omlopp)
- Kortets tillstånd eller status (ej tilldelat, kasserat, oaktiverat, aktiverat, utgånget, spärrat)
- Kortets giltighetstid (tidpunkt då kortet gavs ut, tidpunkt då det aktiverades samt tidpunkt då kortets giltighetstid förfaller)
- Innehavarens namn och person-/samordningsnummer (om kortet är tilldelat)
- Parametrar och värden nödvändiga för att genom ett nollkunskapsbevis verifiera aktiveringskod (för ännu ej aktiverat kort) eller personlig kod (för aktiverat kort).

Registret över innehavare förvaltas av Digg. Leverantörer av identitetsintyg tillåts integrera mot Diggs identifieringstjänst, som är ett applikationsgränssnitt (API) genom vilket en kortinnehavares identitet kan verifieras. Vid verifieringen kontrolleras kortets äkthet, att korrekt personlig kod angivits samt att kortet vid tidpunkten för autentiseringen är giltigt. Svaret som lämnas genom detta API är i princip ett ja eller nej, följt av anledning om svaret är nekande.

Identifieringstjänsten

Kopplat till det register som varje kort och kortinnehavare finns registrerat i, erbjuds en så kallad identifieringstjänst. Detta är den beståndsdel i infrastrukturen som verifierar riktigheten i varje enskild legitimering. Mot denna tjänst interagerar

leverantörer av identitetsintyg, och mot denna tjänst bevisar innehavare av den statliga e-legitimationen sin identitet.

Identifieringstjänsten blir således av stor betydelse för säkerheten i systemet. Det är lämpligt, eller rent av nödvändigt, att skapa diversitet och redundans i denna tjänst för att trygga samhällets försörjning av elektronisk identifiering grundad i den statliga e-legitimationen.

Ett sätt att åstadkomma en sådan diversitet och redundans är att uppdra åt ett antal av de större myndigheterna som har egen it-kompetens och egna driftanläggningar, att var för sig och oberoende av varandra, driva instanser av identifieringstjänsten. På motsvarande sätt behöver det bakomliggande registret också tillhandahållas på ett robust sätt. Samtidigt är dess sårbarheter mindre genom att registret endast exponeras för identifieringstjänsten, medan dess känslighetsgrad är desto större. Registrets riktighet är av avgörande betydelse för säkerheten, innebärande att det måste omges av ett rigoröst skydd, såväl tekniskt som administrativt.

Mot identifieringstjänsten inrättas ett integrationslager. Följande operationer erbjuds av integrationslagret:

- Identifiering
- Underskrift
- Id-växling (användning av e-legitimationen för att skaffa en annan e-legitimation)
- Byte av personlig kod

Integrationslagret bör deklareras med OpenAPI[11] och är ett så kallat HTTP[12] RESTful[13] API. Kommunikation med integrationslagret sker över HTTPS[6] med TLS 1.3[14] över TCP[15] eller QUIC[16] (HTTP/3).

Anrop mellan användaren och integrationslagret stämplas kryptografiskt på meddelandenivå med hjälp av kortets nycklar för kortautentisering genom HTTP Message Signatures[17]. Detta medför dels att anrop endast kan göras tillsammans med

[11] https://www.openapis.org
[12] RFC 9110 – *Hypertext Transfer Protocol (HTTP) semantics*
[13] Representational State Transfer (REST) eller RESTful är ett IT-arkitekturbegrepp som beskriver hur tjänster för maskin-till-maskin-kommunikation kan tillhandahållas genom webbteknik.
[14] RFC 8446 – *The Transport Layer Security (TLS) Protocol Version 1.3*
[15] RFC 9293 – *Transmission Control Protocol (TCP)*
[16] RFC 9000 – *A UDP-Based Multiplexed and Secure Transport*
[17] https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-message-signatures

ett giltigt kort, dels att försök till förändring av meddelanden från användaren kan upptäckas och stoppas.

Även anrop mellan leverantör av identitetsintyg och integrationslagret stämplas kryptografiskt på meddelandenivå, men då av förlitande parts privata nyckelmaterial där motsvarande publikt nyckelmaterial utväxlats via manuella processer.

Autentiseringssessionen

En autentiseringssession mellan användare och förlitande part kan sammanfattas i följande steg:

1. Förlitande part begär åtgärd av något slag av leverantör av identitetsintyg.
2. Leverantör av identitetsintyg skapar en session i integrationslagret. Sessionen innehåller information om vem (vilken förlitande part) som begär identifiering, syfte (identifiering, underskrift eller id-växling) samt annan väsentlig information (t.ex. underlag för underskrift). Skapande av sessionen resulterar i en sessionsnyckel som ska överföras till användaren, t.ex. via en direktlänk eller optisk kod (QR).
3. Användarens klientapplikation ansluter mot integrationslagret, anger sessionsnyckeln och presenterar underlaget för sessionen för användaren.
4. Användaren matar in sin personliga kod samt tillgängliggör sitt kort genom läsaren.
5. Ett nollkunskapsbevis av den personliga koden överförs, kryptografiskt stämplat av kortets nyckel för kortautentisering, till integrationslagret.
6. Integrationslagret genomför kontroller av kortets äkthet och giltighet samt den personliga kodens riktighet, och meddelar leverantör av identitetsintyg resultatet av sessionen.

Klientapplikationer

Kommunikation mellan användaren och centralsystemets integrationslager sker med hjälp av en klientapplikation. Klientapplikationen hanterar kommunikation med användarens kort samt interaktion med användaren, och kan implementeras som en mobilapplikation respektive en applikation för användning i vanlig dator.

Det förväntas att mobilapplikationen är det som i första hand används. Den utformas för att fungera på i princip samtliga förekommande smarttelefoner tillverkade från 2015 (cirka). Mobilapplikationen fungerar endast som ett hjälpmedel att läsa och verifiera kortet, och lagrar således inga uppgifter i telefonens omgivning.

Kommunikationen med kortet (dvs. de datapaket[18] som utväxlas med kortet via det kontaktlösa gränssnittet) tunnlas genom mobilapplikationen till bakomliggande infrastrukturkomponenter som kontrolleras av Digg. Mobilapplikationen tillhandahåller även stöd för att ange den personliga koden, på tidigare beskrivet sätt. Denna kommunikation signeras kryptografiskt med hjälp av kortet, vilket innebär att kort och kod måste föras samman i samma enhet. Kort och personlig kod kan alltså inte hanteras separat, från olika håll.

Identifiering genom mobilapplikationen sker genom att innehavaren antingen erhåller en direktlänk innehållande en referens[19] med sessionsnyckeln för att starta mobilapplikationen, alternativt att mobilapplikationen startas manuellt och sessionsnyckeln avläses från skärmen genom en optisk kod. Sessionsnyckelns giltighet är begränsad i tid, varvid den också kan behöva förnyas med vissa intervall beroende på hur fort användaren reagerar.

[18] Application protocol data unit (APDU) så som detta är definierat i ISO/IEC 7816-4:2020 – *Organization, security and commands for interchange*

[19] RFC 3986 – *Uniform Resource Identifier (URI): Generic Syntax*