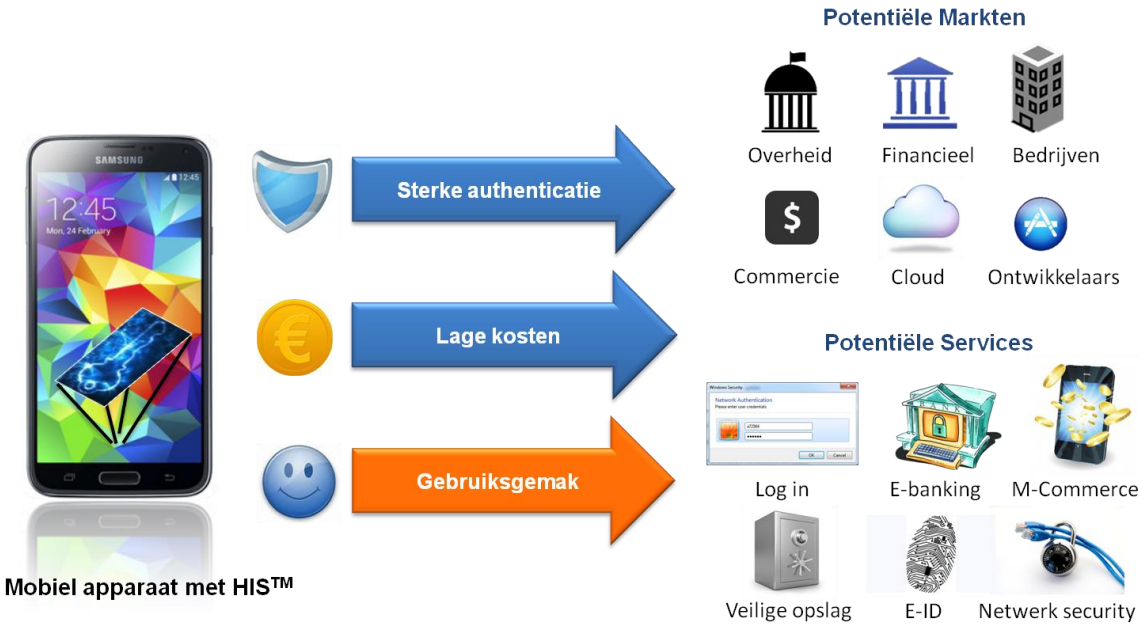
SBIR Cyber security

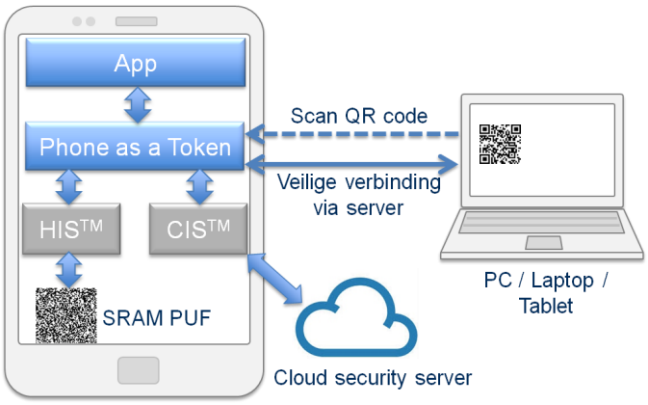
Projecttitel	Bring Your Own Security (BYOS)
Bedrijfsnaam	Intrinsic ID

Projectsamenvatting

Voor steeds meer toepassingen is authenticatie nodig, zoals bij het inloggen op sociale netwerken, bedrijfsnetwerken, telebankieren en webwinkels. Authenticatie is het proces waarbij wordt nagegaan of een gebruiker daadwerkelijk is wie hij/zij beweert te zijn. Hierbij moet de persoon zich uniek identificeren. In veel gevallen wordt dit gedaan met de combinatie van een gebruikersnaam en een wachtwoord. Dit wachtwoord wordt vaak door de gebruiker zelf bedacht. Gebruikers kiezen doorgaans een gemakkelijk te onthouden wachtwoord, terwijl voor de beste beveiliging eigenlijk een zo moeilijk mogelijke letter-/cijfer-/tekencombinatie moet worden gekozen. Bovendien worden wachtwoorden vaak centraal opgeslagen. Hierdoor is deze wijze van authenticatie verre van veilig. Inloggegevens en wachtwoorden worden dan ook veelvuldig misbruikt door cybercriminelen.

Een veiligere vorm van authenticatie is op basis van cryptografische sleutels, welke voor een aanvaller niet te breken of raden zijn. Dit is een groot verschil met inloggegevens en wachtwoorden. Intrinsic ID heeft een technologie ontwikkeld die het mogelijk maakt om deze sleutels op een veilige manier in elektronische apparaten op te slaan. Deze gepatenteerde technologie, genaamd *Hardware Intrinsic Security*™ (HIS), maakt gebruik van unieke eigenschappen van de hardware die bekend staan onder de naam “Physical Unclonable Functions”. Iedere individuele chip heeft een kenmerkend patroon dat in het SRAM-geheugen verschijnt wanneer deze opgestart wordt. Deze “vingerafdruk” is uniek voor iedere chip en komt voort uit minuscule oncontroleerbare afwijkingen tijdens het productieproces. De vingerafdruk is niet aanwezig als de chip uit staat. HIS technologie slaat de authenticatie sleutels op in een nauwe koppeling met deze vingerafdruk. Omdat het patroon van de vingerafdruk onmisbaar is voor het reconstrueren van de authenticatie sleutels wordt het voor een aanvaller onmogelijk om de sleutels uit te lezen of te kopiëren.





Daarom is sleutelopslag met HIS technologie vele malen veiliger dan opslag in bestaande systemen, waarbij sleutels opgeslagen worden in niet-vluchtig geheugen zoals Flash of EEPROM. In dit soort geheugens blijven sleutels aanwezig wanneer het apparaat uitstaat waardoor cybercriminelen ze kunnen uitlezen. Om hier verandering in te brengen gaat Intrinsic ID in dit project HIS-technologie doorontwikkelen en integreren bij minstens één grote en bekende producent van smartphones. HIS technologie zal hierbij gecombineerd worden met een wachtwoord van de gebruiker om op die manier zogenaamde "two-factor-authentication" (dubbele authenticatie) te bieden. Door deze dubbele bescherming, op basis van iets dat de gebruiker weet (wachtwoord) en heeft (sleutel in mobiele toestel), zal deze authenticatie naast gebruiksvriendelijk ook ongekend veilig zijn.

Voor toestellen waarin HIS vooralsnog niet geïntegreerd is (lees: oude smartphones en die van fabrikanten waar Intrinsic ID nog geen contract mee heeft) wordt Cloud Intrinsic Security (CIS) ontwikkeld: een technologie waarbij Cloud services worden gecombineerd met intrinsieke karakteristieken van de smartphone om een sterke sleutel te genereren. Bovenop HIS en CIS zal tevens een 'schil' ontwikkeld worden die het mogelijk maakt dat de sterke sleutels ook op een veilige manier kunnen worden gebruikt in mobiele apps en uitgewisseld kunnen worden tussen smart-phone, PC, laptop, tablet etc. Dit levert uiteindelijk het "Phone as a Token" systeem op dat in bovenstaand plaatje geschetst is en wat het eindresultaat van dit project zal zijn.

Intrinsic ID

Intrinsic ID is marktleider op het gebied van security IP cores en applicaties gebaseerd op gepatenteerde *Hardware Intrinsic Security*™ technologie. Vanuit zijn herkomst uit Philips Research heeft Intrinsic-ID veel kennis en expertise opgebouwd omtrent sterke security oplossingen. Als security bedrijf, heeft het een duidelijke focus op het ontwikkelen van oplossingen voor wereldwijde digitale security problemen. Intrinsic ID's hoofdkantoor ligt in Eindhoven, met verkoopfilialen in San Jose, Tokyo en Seoel.

Contact

Intrinsic ID
High Tech Campus 9
5656AE Eindhoven
+31 (0)40 851 9020
www.*intrinsic-id*.com

Ir. Vincent van der Leest
Senior Project Leader
vincent.van.der.leest@intrinsic-id.com
+31 (0)40 851 9024