Auðkenni ehf.

17.9.2012

AUÐKENNING

- Hver er tilgangur auðkenningar?
- Mismunandi...
  - þjónusta kallar á mismunandi varnir
  - hættur kalla á mismunandi varnir
  - auðkenningaleiðir duga gegn mismunandi hættum
- Hjá fjármálaþjónustu er mikilvægast að koma í veg fyrir svik og ólöglegar millifærslur
- Við aðgengi að viðkvæmum upplýsingum er mikilvægast að vita hver aðilinn er, sbr. heilbrigðisupplýsingar
- Við kosningar, að atkvæði komist til skila með leynd
- Fjöldi árása að aukast, þær eru öflugri og framkvæmdar af öflugum aðilum s.s. glæpasamtökum
- Mörg lög af vörnum nauðsynleg

AUÐKENNI

STORK FULLVISSUSTIG

STORK QAA-fullvissustig				
Fullvissa við **skráningu og afhendingu**			Fullvissa við **rafræna auðkenningu**	
Öryggi ferla við sannvottun kennsla	Öryggi ferla við framleiðslu	Öryggi í starfsemi útgefanda	Öryggi skilríkjanna	Öryggi aðferða við auðkenningu

AUÐKENNI

STORK FULLVISSUSTIG

		Fullvissustig fyrir **rafræna auðkenningu** (*Electronic Authentication – EA*)			
		EA1	**EA2**	**EA3**	**EA4**
Fullvissustig fyrir **skráningu og afhendingu** (*Registration phase – RP*)	**RP1**	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

AUÐKENNI

AUÐKENNINGAR-LAUSNIR

Requirements	Token Type Assurance Levels			
	T1	T2	T3	T4
Password or PIN-based token, chosen by the claimant or automatically generated but not conform common guidelines for strong passwords or PINs (e.g. insufficient length, no mixture of characters, reused, etc.) and therefore vulnerable to guessing or dictionary attacks.	●			
Password or PIN-based token, chosen by the claimant or automatically generated but conform common guidelines for strong passwords or PINs (e.g. sufficient length, mixture of characters, not reused, etc.) and therefore not vulnerable to guessing or dictionary attacks.	●	●		
Soft certificates or one-time password device token.	●	●	●	
Qualified Soft certificates according to Annex I of Directive 1999/93/EC.	●	●	●	
Hard certificates.	●	●	●	
Qualified Hard certificates according to Annex I of Directive 1999/93/EC.	●	●	●	●

AUÐKENNI

AUÐKENNINGAR-LAUSNIR/HÆTTUR

Lausnir/hættur	Online Guessing	Replay	Credential theft	Pharming	Eaves-dropper	Session Hijacking	MITM - wire	MITM - OS	MITB	Transaction Intention	Shoulder-surfing	Keylogging/ Screenlogging
RS + client ssl	4	4	4	4	4	3	4	1	1	2	4	1
RS+lesari m.pinpad + c.ssl	4	4	4	4	4	3	4	2	2	2	4	4
RS+lesari m.skjá + c.ssl	4	4	4	4	4	4	4	4	4	4	4	4
RS+Nexus Sign/auth plugin + ssl	4	4	4	4	4	1	4	3	3	3	4	1
RS á síma OOB + ssl	4	4	4	4	4	4	4	4	4	4	4	4
RS á USB (secure browser)	4	4	4	4	4	4	4	3	4	3	4	1
RS miðlægt + OTP (time) +	4	4	2	4	4	4	4	1	1	1	3	3
RS miðlægt + OTP (seq) +	4	4	2	2	4	4	4	1	1	1	2	2
N/L+OTP(Time) + ssl	4	4	2	4	4	4	4	1	1	1	3	3
N/L+OTP(Seq) + ssl	4	4	2	2	4	4	4	1	1	1	2	2
N/L+SMS+ssl	4	4	2	4	4	4	4	1	1	3	3	3
N/Veflykill+ssl	2	1	1	1	4	1	4	1	1	1	1	1
N/L	2	1	1	1	1	1	1	1	1	1	1	1
Challenge response / with transaction verification	4	4	2	4	4	4	1	1	1	4	3	3
Challenge response	4	4	2	4	4	4	1	1	1	2	3	3

Protection	
1	None
2	Low
3	Medium
4	High

AUÐKENNI

RS - HVAÐ ER BÚIÐ AÐ GERA?

- Lagaumhverfið klárt
- Dreifilyklaskipulagið
  - Uppbygging með samstarfi ríkis og atvinnulífs
    - Hugmyndafræði, þekking, samningar, skjöl, o.fl.
  - Rótin stofnuð (Íslandsrót)
    - Rót rafræns traust í dreifilyklaskipulagi
  - Vottunarstöð Auðkennis
    - Útgáfa ýmiskonar skilríkja fyrir íslenskt samfélag
    - 800 skráningarfulltrúar þjálfaðir, yfir 100 skráningarstöðvar um allt land
- Hægt að nota hjá meirihluta af „mínum síðum“ á Íslandi
- Milli 120-130 þjónustuaðilar styðja auðkenningu
  - Ríki, sveitarfélög, lífeyrissjóðir, fjármálastofnanir, símafélög, tryggingafélög, önnur fyrirtæki, aðrir aðilar og erlendir aðilar
- Endurnýjun debetkorta langt komin

ÍSLANDSRÓT

AUÐKENNI

ÚTBREIÐSLA RAFRÆNNA SKILRÍKJA
HVENÆR KLÁRAST ENDURNÝJUN?

Skilríkjabærir aðilar (15 ára og eldri)	253.292	
Skilríkjabærir aðilar m.debetkort (15 ára og eldri)	226.000	89,2%

		Hlutfall	
	Útgefin kort með skilríkjum	DK	Allir
Heildarfjöldi framleitt (sem eru ekki útrunnin)	286.000	126,3%	112,9%
Þar af virkjuð	101.000	44,6%	39,9%
Framleidd kort (fjöldi einstaklinga)	200.000	88,3%	79,0%
Þar af virkjuð	91.000	40,2%	35,9%

- Endurnýjun debetkorta gengur vel
  - Endurnýjun gæti klárast á næsta hálfa ári
- Virkjunin gengur ekki eins vel
  - Virkjunarhlutfall einstakra aðila (banka eða sparisjóðs) er frá 46% til 95% af afhentum kortum

AUÐKENNI

ÚTBREIÐSLA RAFRÆNNA SKILRÍKJA
HVERNIG GENGUR? SAMANBURÐUR

Country	eID	Mandatory	Eligible citizen	Issued eIDs	Percentag	Rank
Estonia	Identity Card	Yes	1.300.000	1.100.000	84,62%	1
Iceland	**PKI-IS**	**No**	**253.292**	**200.000**	**78,96%**	**2**
Belgium	BELPIC	Yes	9.601.881	7.500.000	78,11%	3
Norway	BankID and more	No	4.985.870	2.730.291	54,76%	4
Sweden	Bank ID and more	No	7.756.200	4.000.000	51,57%	5
Spain	DNIe	Yes	40.000.000	20.000.000	50,00%	6
Italy	CIE & CNS	No	51.000.000	19.500.000	38,24%	7
Germany	Citizen card		70.796.887	10.000.000	14,12%	8
Portugal	Cartão do Cidadão	Yes	10.600.000	1.000.000	9,43%	9
Finnland	FINID	No	4.415.230	350.000	7,93%	10
Slovenia	CSP at the Ministry of Public Administration	No	2.000.000	43.000	2,15%	11
Austria	Bank cards	No	7.000.000	55.000	0,01%	12
	Health insurance card	No	9.000.000	50.000	0,01%	
Denmark	NemID		4.567.805			

AUÐKENNI

RAFRÆN SKILRÍKI

- Skipulag rafrænna skilríkja á Íslandi byggt fyrir hátt öryggisstig
- Árið 2005 óskaði ríkið eftir samstarfi við banka og sparisjóði um almenna útbreiðslu skilríkja á debetkortum
- Íslandsrót var útbúin og markaði kröfur um skilríkin
- Ein megin krafa frá ríkinu var um **fullgild skilríki**, sbr. lög
- Fullgild skilríki gera m.a. kröfu um að einstaklingar mæti á staðinn og sanni á sér deili við virkjun skilríkja
  - Fá meirihluta þjóðarinnar á staðinn tekur tíma...(mörg ár)
  - ...gerir kröfu um ferðalög og tíma almennings
  - og kostar fjármuni fyrir útgefendur skilríkjanna...
  - ...en þarf ekki að gera oft (rafræn auðkenning eftir það)

AUÐKENNI

RAFRÆN SKILRÍKI HJÁ RÍKINU

- Ein af hindrunum fyrir frekari þróun í rafrænni stjórnsýslu hefur verið talin skortur á almennri útbreiðslu rafrænna skilríkja
- Forsenda fyrir aðgengi að viðkvæmum upplýsingum
  - Heilbrigðisupplýsingar
  - Málaskrá lögreglunnar
- Forsenda fyrir rafrænum kosningum
- Forsenda fyrir rafrænum undirskriftum
- Almenn útbreiðsla rafrænna skilríkja hefur verið forgangsverkefni hjá Evrópusambandinu og ríkjum í Evrópu

- Á ÞETTA EKKI LENGUR VIÐ?

AUÐKENNI

INNLEIÐING RAFRÆNNA SKILRÍKJA

Hvað er búið

- Búið að byggja upp grunnskipulag
- Endurnýjun debetkorta með rafrænum skilríkjum á lokastigum
- Rafræn skilríki orðin vegabréf í netheimum
  - Færri notendanöfn og lykilorð (yfir 120 þjónustur)

Hvað er eftir

- Framkvæma úrbætur til þess að auðvelda afhendingu,virkjun og notkun skilríkjanna
- Stuðningur við nýtt umhverfi (spjaldtölvur og snjallsímar)
- Þjónustuaðilar nýti kerfið betur og bjóða þær þjónustur sem skilríkin eru talin forsenda fyrir
- Kynna ábata rafrænna skilríkja
- Auka notkun...

AUÐKENNI

SPURNINGAR

- Mun ein leið hafa vinninginn og verða notuð hvarvetna þar sem auðkenningar?
  - EIN LEIÐ MUN VERÐA RÁÐANDI, sbr. BankID og NemID (Norðurlönd)
- Er þörf á mörgum auðkenningarleiðum?
  - ???...margar lausnir verða notaðar til stuðnings við auðkenningu
  - bankar munu t.d. nota, fraud detection, risk-based authentication, transaction monitoring, device and behavioral identification, Out of band, SWYS (see what you sign)
- Verða margar auðkenningarleiðir notaðar samhliða
  - JÁ (EINNIG SAMA GRUNNLEIÐIN MEÐ VIÐBÓTAR RÁÐSTÖFUNUM)
- Eftir því hversu mikils öryggis verður krafist?
  - JÁ
- Munu ný tæki og tækni hafa áhrif á auðkenningarleiðir í náinni framtíð?
  - JÁ, SÉRSTAKLEGA NÝ TÆKNI ER VARÐA NÝJAR ÓGNIR (ÁRÁSIR)

AUÐKENNI

RAFRÆN SKILRÍKI

- Á ÍSLANDI ER NÚ ALMENN ÚTBREIÐSLA RAFRÆNNA SKILRÍKJA
- FÖRUM NÚ AÐ NÝTA OKKUR SKILRÍKIN…
- …OG STUÐLUM AÐ ALMENNRI NOTKUN

AUÐKENNI