Lessons from Directive 1999/93/EC

Paweł Krawczyk
pawel.krawczyk@hush.com

Complete requirements?

- (4) Electronic communication and commerce **necessitate** "electronic signatures" and related services allowing data authentication
  - Where is communication & commerce now?
    - Do they use QES?
  - Did we really ask commerce?
    - Yes – we delivered something else
    - No – we got what we deserve

(8) **Rapid** technological development

T0 1999 Directive

T+5 2004 CEN still working on CWA

T+10 2009/767/EC
Single point of contact, TSL
„risk assessment" !

T+12 2011/130/EU
Reference ES format
Public consultation on 1999/93/EC

(FORECAST)

2012-2020 Reports, analyses, conferences, meetings…

WHO NEEDS 80'S TECHNOLOGY IN 2020?

Differentiated services

- (20) …national law lays down **different requirements for the legal validity of hand-written signatures**; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a **higher level** of security;
  - Why is it important?

Compare E-banking

	# of banks	Sector preferences	
Authentication method		**Consumer**	**Corporate**
SMS	15	Ease of use, adequate security	Repudiation
Hardware OTP token	11	High TCO	Higher security, some non-repudiation
Printed OTP list (TAN)	7	Basic security	Repudiation
Digital signature (*)	2	High TCO, difficult to use	High non-repudiation
Static password	0	2011 – insecure 2000 - enough	2011 – insecure 2000 - enough

(*) Not neccessarily QES

Source: Michał Macierzyński, „Najbezpieczniejsze banki internetowe w Polsce”, Bankier.pl, 2009

80's security assumptions

*„A typical environment (…) might be **the home or the office**, where the individual or the company has direct control of the SCS (Signature Creation System)"*

- A typical pre-Internet assumption!
- No difference between „home or office" in the Internet
- Solution from QCAs: „use antivirus"

Source: CWA 14170:2004, section 5.6

Does it work?

File name:	**facebook-pic00049232016.exe**
Submission date:	**2011-09-14 22:41:25 (UTC)**
Current status:	**finished**
Result:	**11 /44 (25.0%)**

Compact

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.09.14.00	2011.09.14	-
AntiVir	7.11.14.204	2011.09.14	-
Antiy-AVL	2.0.3.7	2011.09.14	-
Avast	4.8.1351.0	2011.09.14	Win32:Ruskill-CU [Trj]

Why projects fail?

- **Incomplete Requirements**
- **Lack of User Involvement**
- Lack of Resources
- **Unrealistic Expectations**
- **Lack of Executive Support**
- Changing Requirements & Specifications
- Lack of Planning
- **Didn't Need It Any Longer**
- Lack of IT Management
- **Technology Illiteracy**

Source: The Standish Group, „Chaos Report", 1995