Technology Trends in eID

March 7, 2017

Jeremy Grant
Managing Director
The Chertoff Group

eID is changing

The market has evolved significantly over the last few years, driven by new:

- Technology innovations
- Standards
- Business models
- Government initiatives

eID is changing

The Old Way

- Passwords are “good enough”

Today

- Passwords are at the heart of nearly every major breach.

- Password stores and security questions are a frequent target – since people reuse them across sites
  - **71%** of accounts are protected by a password that is being reused across multiple accounts
- Facebook: “**600,000 logins** compromised each day”

Breach	Date	Attack Vector
Yahoo	Dec. 2016	Multiple (target was passwords and answers to authentication “security questions”)
DNC	Jul. 2016	Compromised Passwords
OPM (2 Breaches)	May 2015	Compromised Password
Anthem	Feb. 2015	Compromised Password
IRS	May 2015	Inadequate Authentication (compromise of “knowledge-based” questions)
JP Morgan Chase	Jul. 2014	Compromised Password
Target	Dec. 2013	Compromised Password
Apple iCloud	Aug. 2014	Compromised Passwords
Home Depot	Sep. 2014	Compromised Password
Sony Pictures	Dec. 2014	Compromised Password
Heartbleed	Apr. 2014	Bug Exposing Passwords
1.2 Billion Passwords (Russian CyberVor Hacker Gang)	Aug. 2014	Multiple (target was passwords to be used for other potential attacks)

eID is changing

The Old Way

- eID means I have to issue a card.

Today

- Everybody carries something in their pocket that offers all the capabilities of the card – and more.

Trusted Execution Environment (TEE), SIM, or Secure Enclave (SE)

Multiple Biometric Sensors (finger/face/iris/voice)

NFC, 4G and Bluetooth

It's not a "Phone" – it's a multi-factor cryptographic token

eID is changing

The Old Way

- Multi-Factor Authentication (MFA) is too hard/expensive/cumbersome

Today

- MFA is built into your device – enabled by FIDO Alliance standards – and it's easier to use than passwords

Key Authentication Elements

Biometric

+

Public Key Cryptography

More than 300 FIDO-certified products – up 200% YoY

Implications for eIDAS

- FIDO offers an option to extend the trust model of a country's traditional eID – allowing the eID to more easily be used to in a wider array of applications.
  - Why? Commercial service providers are less likely to integrate with a particular country's eID than they are with a global standard like FIDO.

  - A FIDO keypair derived from an eID can allow it to be used in more places

- Conversely, eIDs under eIDAS can be used to help with commercial identity proofing, validated attributes, and account recovery

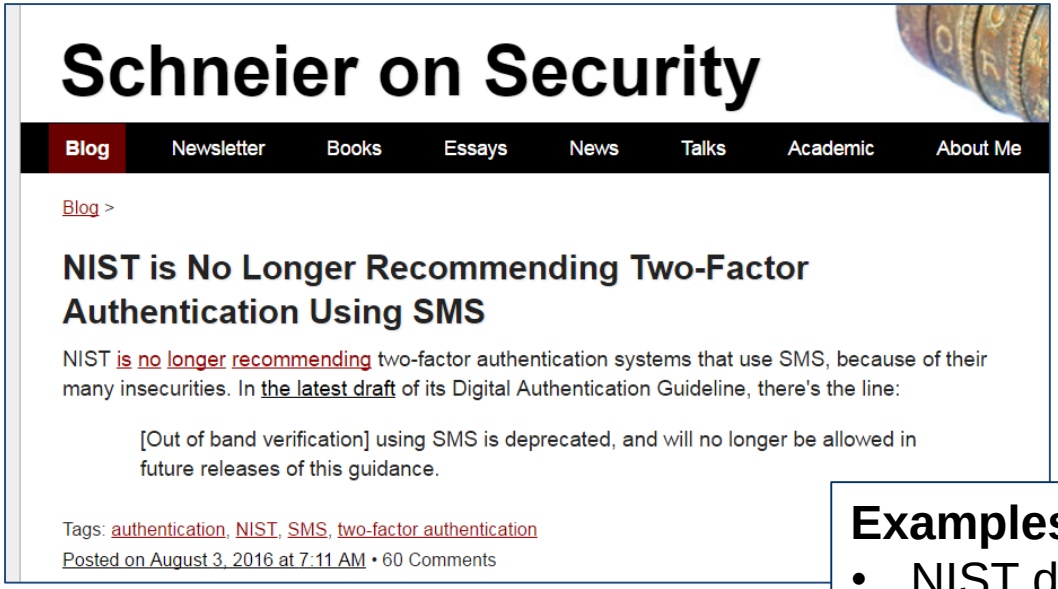
eID is changing

The Old Way

- All MFA is the same.

Today

- MFA based on shared secrets is increasingly vulnerable.



Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks | Academic | About Me

Blog >

NIST is No Longer Recommending Two-Factor Authentication Using SMS

NIST is no longer recommending two-factor authentication systems that use SMS, because of their many insecurities. In the latest draft of its Digital Authentication Guideline, there's the line:

> [Out of band verification] using SMS is deprecated, and will no longer be allowed in future releases of this guidance.

Tags: authentication, NIST, SMS, two-factor authentication

Posted on August 3, 2016 at 7:11 AM • 60 Comments

Examples

- NIST deprecation of SMS (SP 800-63)
- NIST downgrading of OTP to AAL2 based on inferior “Verifier Impersonation Resistance” (SP 800-63)
- Google statements on OTP hacks (2015)

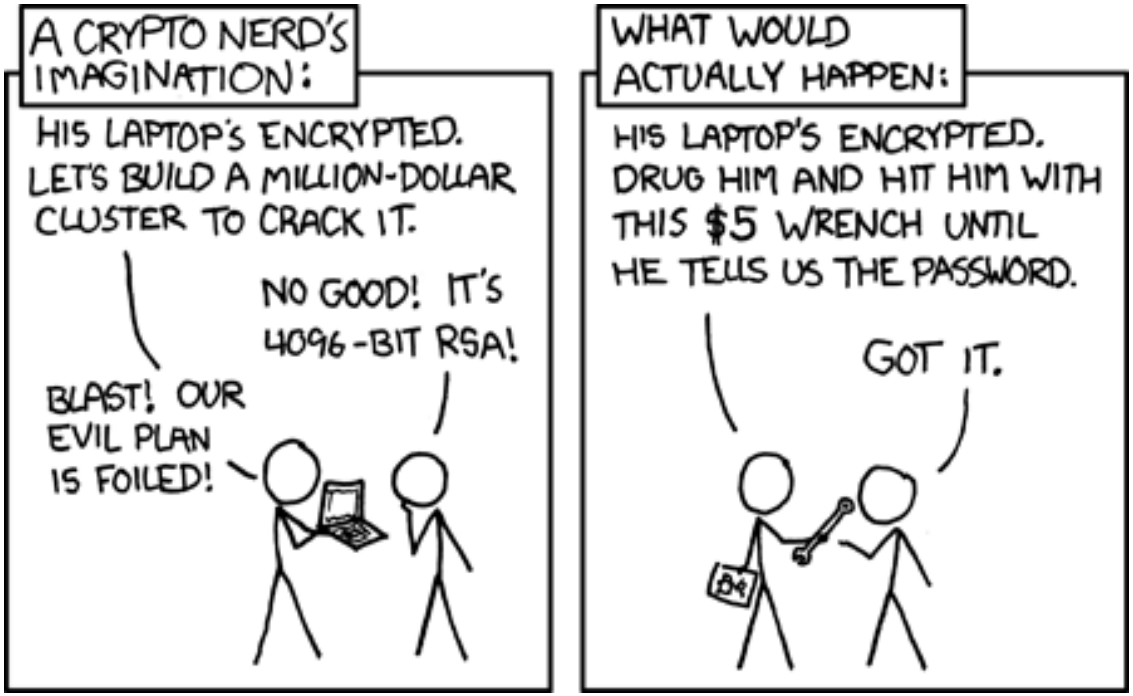
eID is changing

The Old Way

- It's all about Security.

Today

- It's about better customer and citizen experiences.



Source: *xkcd*

Usability

Privacy

Interoperability

Liability

Business Models

eID is changing

The Old Way

- Social Login is about convenience, not security.

Security

Your Facebook account is now more secure than your bank's (probably)

Protect those baby pics and political rants with hardware two-factor auth keys

26 Jan 2017 at 19:40, John Leyden

Facebook is upgrading its login defenses by rolling out support for hardware security keys.

The move means that Facebook addicts can make their logins far more resistant to phishing and account hijackings – and makes the site more secure than banks' online services that provide just single-factor authentication.

Users can log into Facebook by tapping on a USB key connected to their computer after entering th password. That key is paired with the netizen's Facebook account and emits a special string to the social network, via the browser, that authorizes the login.

So if a crook learns your password, that information is no good without your physical two-factor authentication key. Facebook offers two-factor authentication via text messages, but this isn't as reliable or secure as a separate hardware token.

FIDO-compliant Universal 2nd Factor (U2F) keys cost £16.00 ($20) from the likes of Amazon's marketplace and Yubico. NFC-capable keys can be paired with compatible mobile devices for mobile

Today

- Don't look now, but…

AMERICAN BANKER All Sections

NOW READING: The Latest | Why banks should consider taking a page from Facebook … | SoFi-Zenbanx deal accelerates fintech convergence trend | KYC vs. data privacy: Can this fintech thread the needle? | How fintech c problem unde

Why banks should consider taking a page from Facebook on security keys

By
Bryan Yurcan

Published
January 26 2017, 6:22pm EST

More in
Authentication
Identity verification
Cybersecurity
Online banking
Bank technology

Print | Email | Reprints | Share

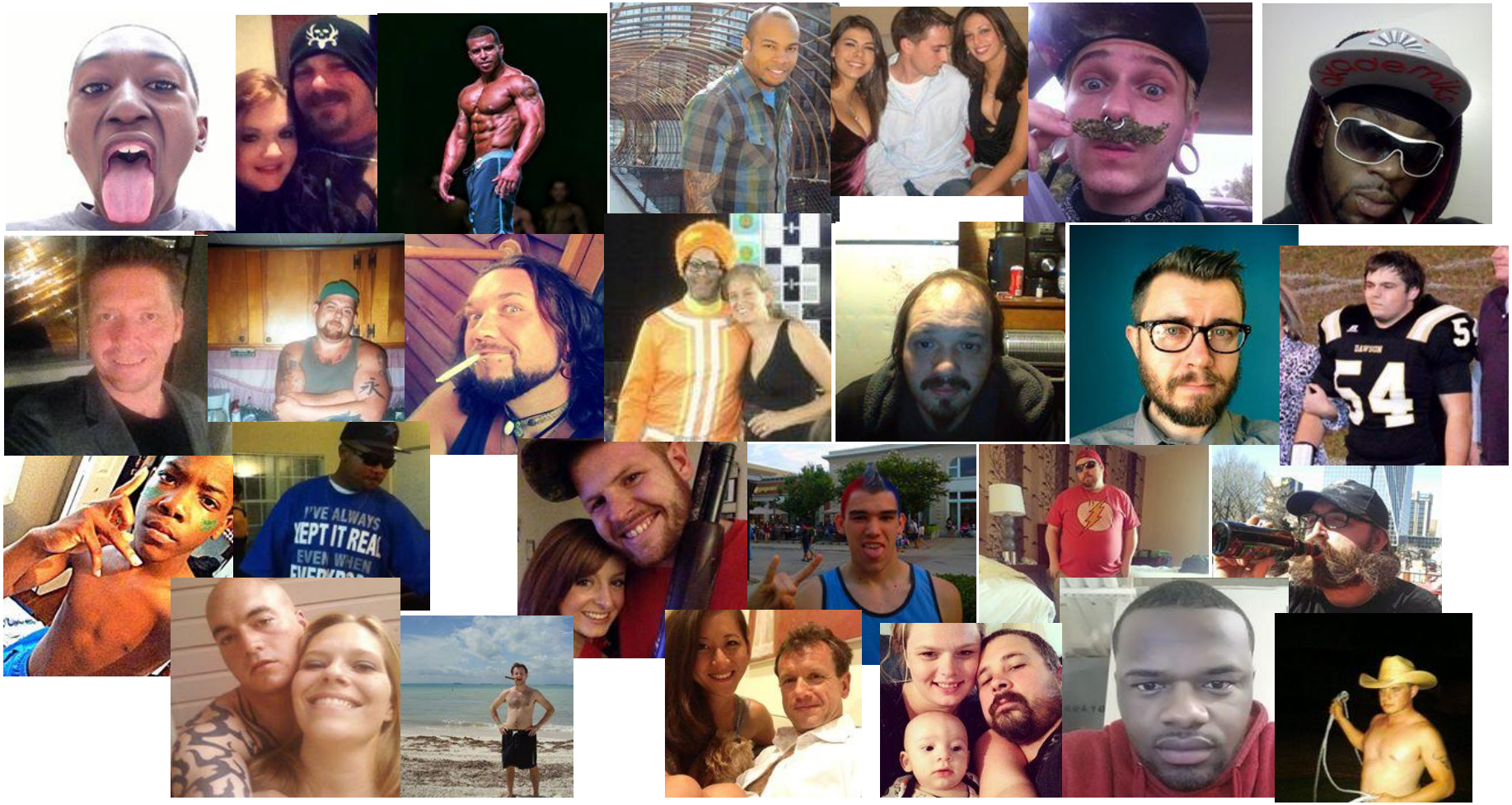
If Facebook brings physical security keys to the masses, is it time for online banking to finally adopt them too?

Facebook announced Thursday it is giving its users the option of authenticating with hardware security keys that meet the standards of the Faster Identity Online Alliance. These devices are typically the size of a thumb drive and can be plugged into the USB drive of a desktop computer. When logging in, after typing in their passwords, users would press a button on the device as a second factor of authentication.

Banks have long offered similar physical authentication devices to larger commercial clients, but rarely if ever to retail customers. The second factor of authentication is more likely to be a one-time code sent via email or text message.

eID is changing

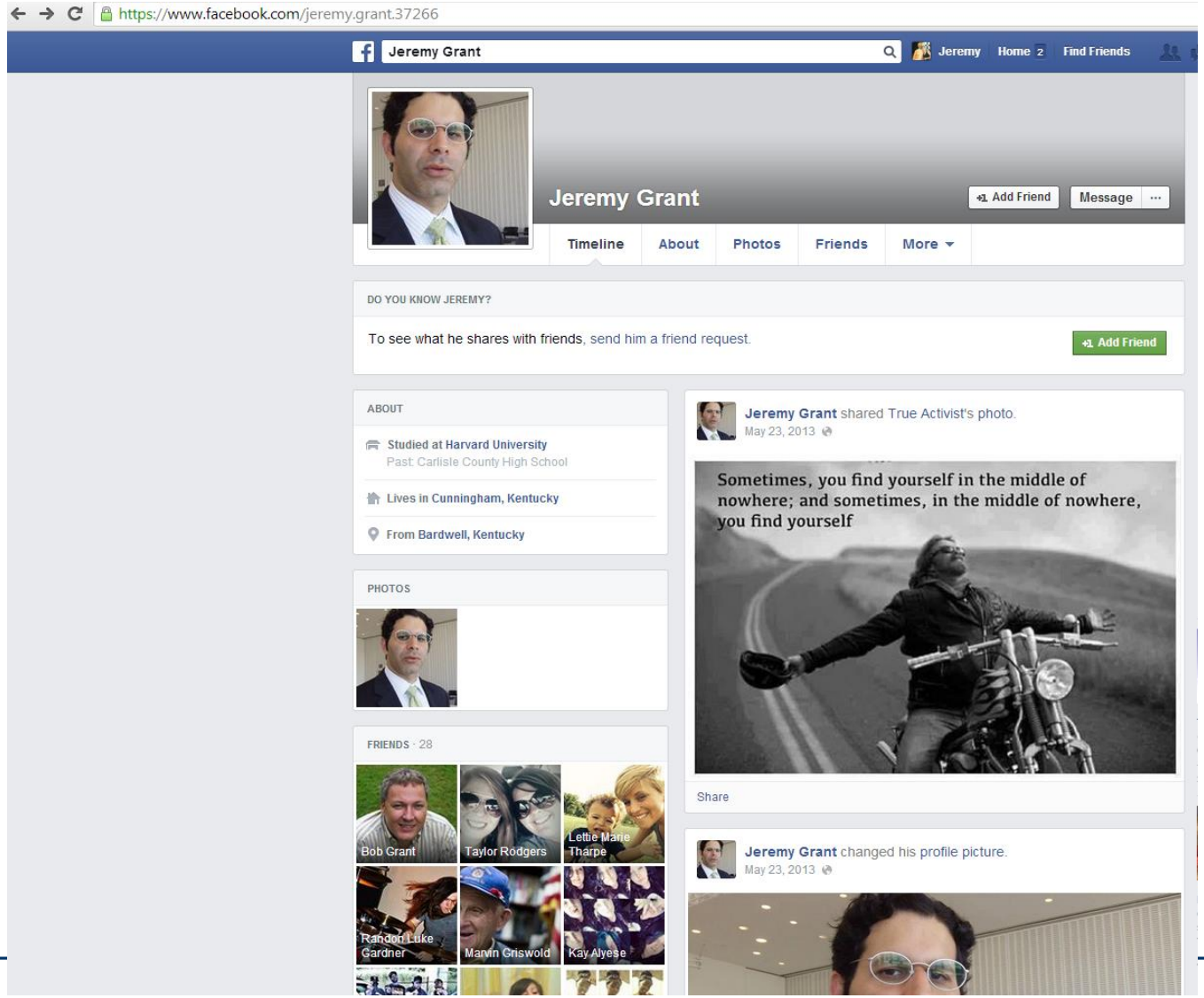
Although there are still some issues to work out



"Jeremy Grant" on Facebook

eID is changing

Although there are still some issues to work out (this is not me)



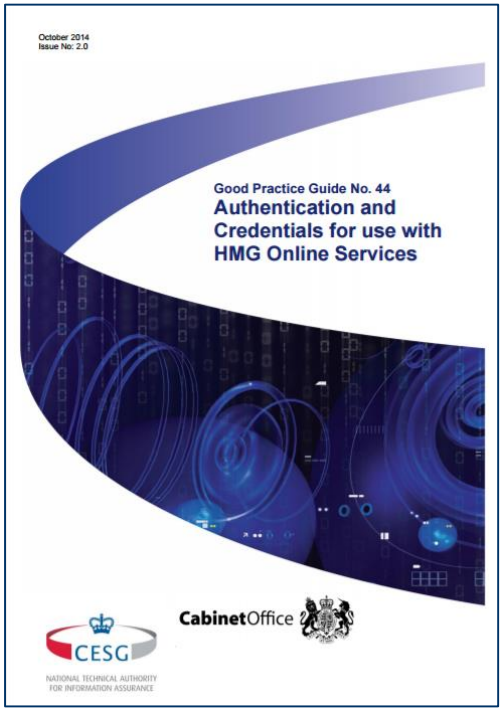
eID is changing

The Old Way

- Each country has its own eID scheme, hard to map between them

Today

- Beyond eIDAS – countries are actively collaborating, looking for opportunities to harmonize




COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Almode Networks
Los Altos, CA

Elaine M. Newton
Office of the Director
Information Technology Laboratory

Ray A. Perlner
Computer Security Division
Information Technology Laboratory

Andrew R. Regenscheid
Computer Security Division
Information Technology Laboratory

William E. Burr
Dakota Consulting, Inc.
Silver Spring, MD

Justin P. Richer
Bespoke Engineering
Billerica, MA

Privacy Authors:

Naomi B. Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

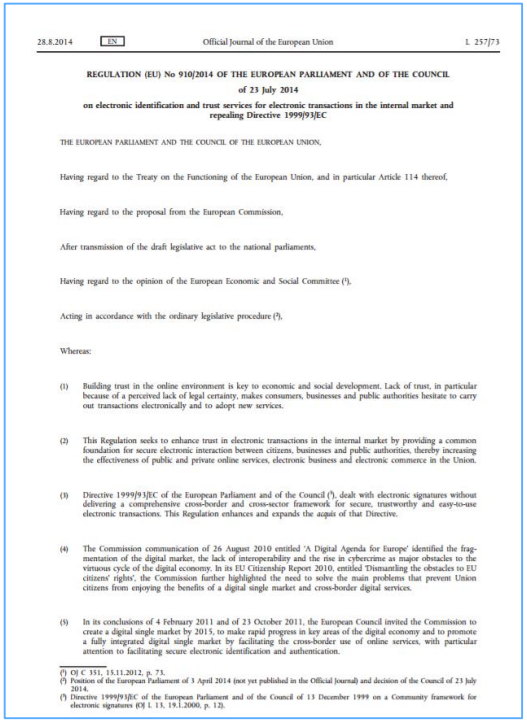
Jamie M. Danker
National Protection and Programs Directorate
Department of Homeland Security

Usability Authors:

Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos
Information Access Division
Information Technology Laboratory

Month TBD 2017

National Institute of Standards and Technology
Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology and Director


28.8.2014 EN Official Journal of the European Union L 257/73

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 23 July 2014
on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

(3) Directive 1999/93/EC of the European Parliament and of the Council (3), dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the acquis of that Directive.

(4) The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.

(5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(1) OJ C 351, 15.11.2012, p. 73.
(2) Position of the European Parliament of 3 April 2014 (not yet published in the Official Journal) and decision of the Council of 23 July 2014.
(3) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

eID is changing

Although there are still some issues to work out

Thoughts on International Collaboration on eID

There are opportunities between the US and Europe – but they will be driven more by commercial interests than government

- At the government level, it was already hard before the election; with the “America First” shift – do not expect the new U.S. Administration to make this a priority
- The private sector does care about cross-border identity – and has a number of incentives to do so
- New and better standards and trust frameworks – which did not exist 5 years ago – make this easier
- Examples
  - A FIDO U2F token issued to a UK citizen as part of GOV UK Verify can also be used to log in at Google, Facebook, GitHub, Dropbox, etc.
  - Banks on both sides of the ocean are increasingly looking at opening up their consumer identity solutions to other parties
  - Efforts by US/UK to harmonize identity standards (NIST SP 800-63-3 and UK GPG 44)

Thank you!

jeremy.grant@chertoffgroup.com