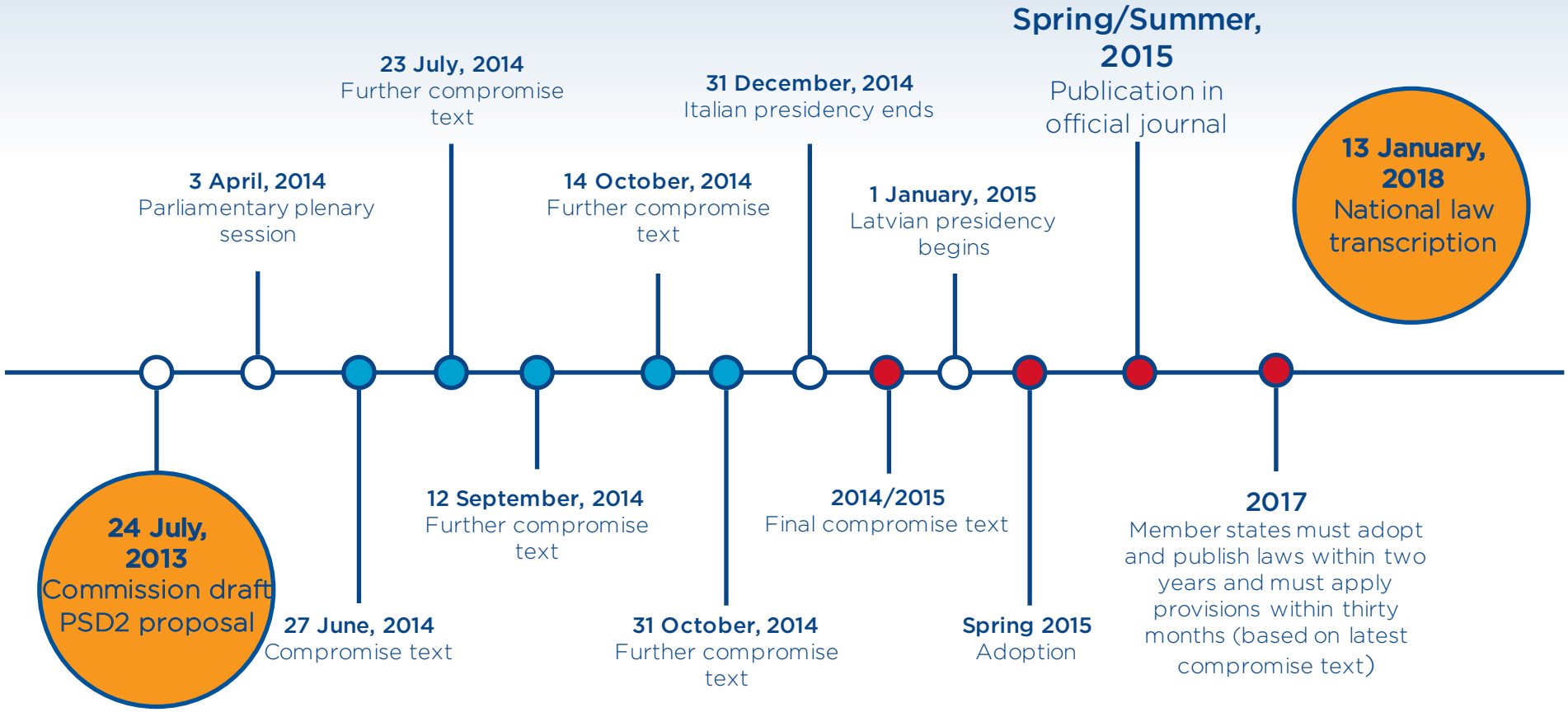
PSD2:
Risks, Opportunities and New Horizons

Contents

Timeline


24 July, 2013
Commission draft PSD2 proposal
3 April, 2014
Parliamentary plenary session
27 June, 2014
Compromise text
23 July, 2014
Further compromise text
12 September, 2014
Further compromise text
14 October, 2014
Further compromise text
31 October, 2014
Further compromise text
31 December, 2014
Italian presidency ends
1 January, 2015
Latvian presidency begins
2014/2015
Final compromise text
Spring 2015
Adoption
Spring/Summer, 2015
Publication in official journal
2017
Member states must adopt and publish laws within two years and must apply provisions within thirty months (based on latest compromise text)
13 January, 2018
National law transcription
Trilogue discussions and ordinary legislative procedure

Implications

Implications

Strong authentication and secure communications

Knowledge

Possession

Inherence

Implications

Third party provider (TPP) regulations

AISPs (Account Information Service Providers)

Consumers are enabled to track and analyse their financial data

PISPs (Payment Initiation Service Providers)

Consumers are empowered to use any PISPs for their online payment accounts

Implications

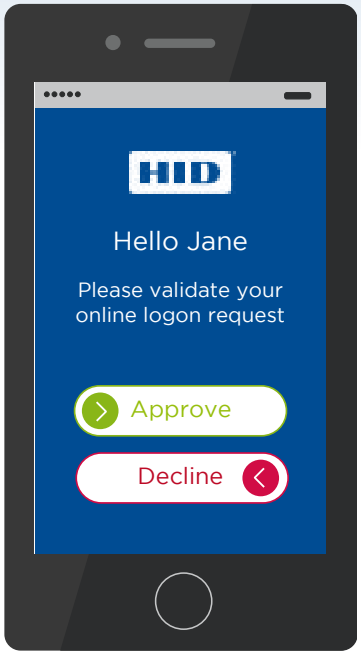
Access to account' element (XS2A)

Banks **must allow access** to their customers' account information **to facilitate payment initiation and account information services**, provided by TPPs while **offering the best deals** to their existing clients.

Implications

Platformification of the bank

> The revised PSD2 provisions have accelerated the competition and disruption of the financial services industry. Consequently, **the financial services industry's interest in Open APIs and Open Banking is gaining momentum and is not limited to payments.**
>
> Euro Banking Association Working Group on Electronic Alternative Payments



HID Global empowers banks to federate the legacy banking systems to support the Open Banking API initiative - based on industry standard open APIs.

Unrivalled Security

Unrivalled Security

> The **confidentiality, authenticity and integrity** of the information displayed to the user through all phases of the authentication procedure including **generation, transmission and use** of the authentication code.

Information sent through secure channels

Data encryption and message integrity check

Segregated communication channels

Unrivalled Security

> The payer is made aware of the **amount of the payment transaction and of the payee**; the authentication code generated shall be **specific to the amount of the payment transaction and the payee** agreed to by the payer when initiating the transaction.

Secure and segregated channels

Confidentiality of authentication information must be protected

Transaction information displayed to the user

The user is in control and in perfect knowledge when approving a transaction

Transaction Signing

Transaction is verified and approved

Enriched Customer Experience

Enriched Customer Experience

In-person authentication

Instant validation

Control over risk

> The **payer is made aware at all times of the amount** of the transaction and of the payee. The **generated must be specific to the sum of the transaction** and agreed to by the payee when initiating the transaction.

Enriched Customer Experience

Bank with confidence

Trusted beneficiaries definition

Customers can confidently define new beneficiaries.

Banks are guaranteed that all beneficiaries are approved by the customer.

> The application of **strong customer authentication shall not be exempted** where the payer creates for the first time or subsequently amends the list of trusted beneficiaries with its account servicing payment services provider.

Absolute Trust

Absolute Trust

> Strong authentication... **is always traceable back to an individual or company.**

RASP (Runtime Application Self Protection)

Empower organisations to identify secure, safe and trusted devices.

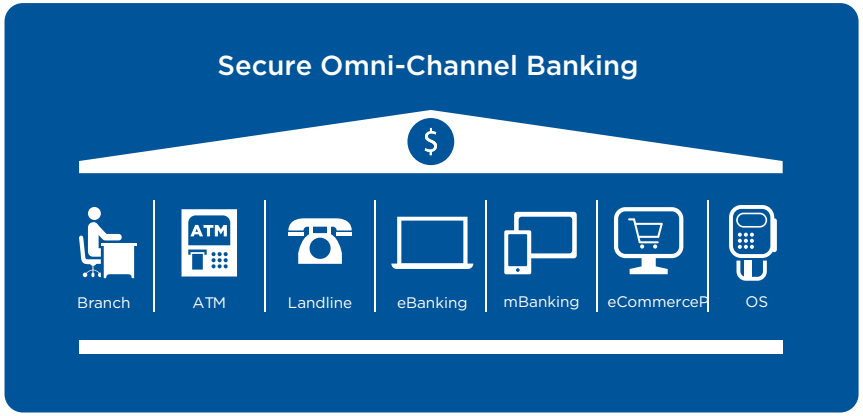
Real-time location analysis

Enable organisations to determine the location of the device accurately.

Instant user identification and authentication

Leverage the benefits of behaviour metrics to verify who the person using the authentication is, in fact, the customer.

Absolute Trust



HID Adaptive Security Approach	PSD2 Strong Customer Authentication
Application security	**Replication prevention**
Transactional signing and pattern-based intelligence	**Dynamic linking**
Browser protection **Device authentication**	**Confidentiality, authenticity, data integrity**
User authentication (MFA) Something **you know** *(passwords)* Something **you have** *(token)* Something **you are** *(biometrics, behaviour metrics)*	**User authentication (MFA)** **Knowledge** *(passwords)* **Possession** *(token or tokenless)* **Inherence** *(biometrics, behaviour analytics)*

Absolute Trust

Added Value Services

High strategic value to your investment

Industry leading experts to enable end-to-end solutions

Integration assistance on larger scale projects

Deployment assistance and training to give you the tools

Customisation and configuration

Consultation

Integration

Training

Listen to our webinar on demand for further insight how to meet the regulatory requirements

Contacts

HID Global
North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

hidglobal.com

An ASSA ABLOY Group brand

ASSA ABLOY