Gemalto – The PSD2 Expert Company

PSD2 compliant means for your authentication needs

Compliancy with PSD2 is one of the most important challenges for banks in this decade and Gemalto is fully committed to support its customers on this journey.

Technology Gemalto has developed over the past two decades for **Strong Customer Authentication** and **Risk-Based Authentication** is a great benefit for all financial institutions, in both, to cope with new regulations as well as tackle the new business opportunities PSD2 enables with various new players in the ecosystem.

Whether you look for mobile, hardware or risk-based authentication solutions, Gemalto can be your provider for all of those with its PSD2 compliant portfolio. To simplify your journey, Gemalto has also its cloud-based ID Cloud offer which will be the easy and secure way for you to solve your authentication needs using a cloud-based suite of Gemalto authentication solutions.

Let our team to help you with your PSD2 related concerns.

Mobile authentication as preferred option

What modern end-users really want to use these days is mobile solutions. Whether it is an online purchase, social media interaction, stock purchase or accessing online bank, it needs to be available via Mobile. And the same goes for authentication.

Gemalto Mobile Protector is a field-proven technology trusted by leading banks and financial institutions globally to secure financial mobile applications while providing great user experience.

Available in iOS and Android, with biometrics support and built in Gemalto technology to provide highest level of security, it is a true turn-key solution for banks looking for PSD2 compliant mobile authentication.

PSD2 and compliance of our mobile solution towards the RTS is vital for us. We have implemented all required security mechanisms and workflows which are required to make our Mobile Protector and powerful tool to help you to reach compliancy with PSD2. The table below illustrates different requirements of the RTS for mobile solution.

MAIN REQUIREMENTS	RTS ARTICLE	COMPLIANCY
Separated environments	Recital 6, Article 9	✓
Protecting data	Recitals 18, 26,..., Articles 1, 5, 22	✓
Secure communications > Credentials generation and transmissions > Secure data transmissions	Recitals 18, 26,..., Articles 1, 5, 22	✓
Device and software integrity	Recital 6, Article 9	✓
Two-Factor Authentication	Recital 6	✓
Security and independence of the authentication elements	Recital 6 Article 9	✓
Dynamic linking	Recitals 3, 4 Article 5	✓
Data Confidentiality and Integrity	Recitals 2, 18, 26,..., Articles 1, 5, 22	✓
Secure onboarding	Article 24	✓
Protecting the knowledge factor	Article 6	✓
Protecting the possession factor	Article 7	✓
Protecting the inherence factor	Article 8	✓

Hardware tokens to back-up

Eventhough Mobile is truly a channel for majority of the consumer to go with, it will not be a solution that covers all users. Some people prefer to stick with more traditional means and want to avoid making everything "so mobile". In particular this is the case for retail users not having a smartphone or corporate users willing to manage security outside of their mobile phones. Also, in order to provide a fallback solution in case when mobile is stolen some other means of authentication is important. Gemalto's answer to this is user-friendly, secure, PSD2 compliant, hardware based authentication tokens. Used globally by most of the financial organizations they are powerful and cost effective way to address all user groups without giving anything away in terms of security. In the table below you will see what requirements in the RTS are relevant in case of hardware tokens and you will see how Gemalto hardware tokens comply.

MAIN REQUIREMENTS	RTS ARTICLE	COMPLIANCY
Two-Factor Authentication	Recital 6	✓
Security and independence of the authentication elements	Recital 6 Article 9	✓
Dynamic linking	Recitals 3, 4 Article 5	✓
Data Confidentiality and Integrity	Recitals 2, 18, 26,..., Articles 1, 5, 22	✓
Secure onboarding	Article 24	✓
Device and software integrity and authenticity	Recital 6, Article 9 Article 25	✓
Protecting the knowledge factor	Article 6	✓
Protecting the possession factor	Article 7	✓

Risk-Based Authentication bringing user convenience

Imagine user experience where online banking systems would be able to distinguish good users from the fraudsters before the transaction or strong customer authentication would even take place. This would be a great way to show appreciation towards your loyal customers. In order to enable this, and take the full benefit of exemptions given by PSD2 and the RTS, your solution is Gemalto Assurance Hub. With the combination of world leading fraud detection systems and single, unified API to access them, it will take financial institutions a leap forward in their customer satisfaction and reduction of cost related to fraud. Following table illustrates the definitions of RTS which are relevant for the risk-based authentication solution and shows you for which of them Gemalto Assurance Hub (GAH) will comply.

RISK FACTORS TO MONITOR / INFORMATION TO ANALYZE	RTS ARTICLE	GAH COMPLIANCY
Abnormal spending and behavioral pattern of the payer	18.3	✓
Unusual information about the payer's device/software access	2.2	✓
Malware infection in the authentication procedure	2.2	✓
Unauthorized and fraudulent payment transactions	2.1	✓
Location of the Payer and Payee	18.3	✓
Transaction history of the user	18.3	✓
Log of the use of access device or the software	2.2	✓
Perform real-time risk analysis and provide risk scoring	18	✓
Separate low-risk and high-risk transactions and apply exemptions	18	✓

ID Cloud offer banks a fast track to PSD2 compliancy

Banks in Europe face very short deadlines to achieve PSD2 compliance and their IT departments may have to commit significant time and resources to deploy and maintain the solutions required to meet them. ID Cloud offers a fast and efficient alternative to comply with PSD2. ID Cloud is Gemalto's cloud-based, managed service offer for Banks to cover all their Risk-Based and Strong Customer Authentication needs. It offers the same technology as presented above but the backend components are managed in the cloud by our expertized operation teams. We grant PSD2 compliance of our implementation, very fast project deployment compared to an on-premise set-up, highly reliable and scalable IT infrastructure and a transaction based commercial model that meets the needs of large and smaller banks alike.

GEMALTO.COM

gemalto
security to be free