FULLY TRUSTED AUTHENTICATION

A LAYERED APPROACH TO SECURITY GUARANTEES:
- Optimized Risk Mitigation
- Secure Mobility
- Peace of Mind

To have a fully trusted authentication environment, enterprises must assure their authentication solution is built on a solid foundation.

5 pillars of a Fully Trusted Authentication Environment

1. Standard Based Protocols
   - Solutions based on international encryption and authentication standards ensure transparency and business confidence.

2. Protecting Authentication Data
   - Token secrets can be programmed dynamically in the field, giving customers control over their authentication data at all times.

3. Certifications
   - Solutions that are audited and validated by 3rd party organizations meet the highest security standards.

4. Hardware Based Root of Trust
   - A hardware-based root of trust mitigates the risk of the key being compromised.

5. Choice of Tokens
   - A choice of authentication methods and token formats ensures risk optimization for different use cases.

SafeNet continuously invests efforts and resources in providing customers with a Fully Trusted Authentication environment driven by:
- Ensuring that our authentication solutions comply with international and regional certifications and regulations.
- Ensuring our products are based on internationally recognized encryption standards and protocols.
- Providing customers with full control over their authentication data.
- Securing our authentication solutions with a hardware-based root of trust.