Product Evaluation Report

Smarter Authentication Platform from Encap Security

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

ENCAP®
SECURITY

CONTENTS

This is a Product Evaluation Report from Goode Intelligence of Encap Security's Smarter Authentication Platform. It provides an independent evaluation of Encap's authentication platform based upon Goode Intelligence's expertise of the authentication and identity management market.

COMPANY OVERVIEW

Encap Security (Encap AS) is a privately owned and funded multi-factor authentication technology vendor headquartered in Oslo, Norway, with offices in Palo Alto, USA.

The company is venture-backed and is led by Thomas Bostrøm Jørgensen, Chief Executive Officer (CEO).

Encap provides strong multi-factor authentication (***MFA***) and digital signing solutions aimed at financial and enterprise sectors through its ***Smarter Authentication Platform***.

The multi-factor authentication solution is mobile–based and leverages the built-in capabilities of ***smart mobile devices*** (***SMD***); offering a frictionless authentication experience that is both easy to use and secure.

HIGH-LEVEL PRODUCT DESCRIPTION

Encap's Smarter Authentication Platform provides device-based strong authentication and ***e-signature*** solutions.

The software platform is aimed at industries that require strong, internet-scale authentication, and can be run within their own infrastructure; making it particularly suitable for financial services and other regulated industries.

The device-based authentication solution combines ***risk-based authentication***, ***flexible authentication-factor choice***, ***malware detection***, ***jailbroken/rooted device detection and protection, and support for the latest biometric authentication solutions including Apple Touch ID***.

Goode Intelligence Product Evaluation Report

GI's Product Evaluation Report's (PER) offer an independent analysis of cybersecurity products and services.

GI Definitions

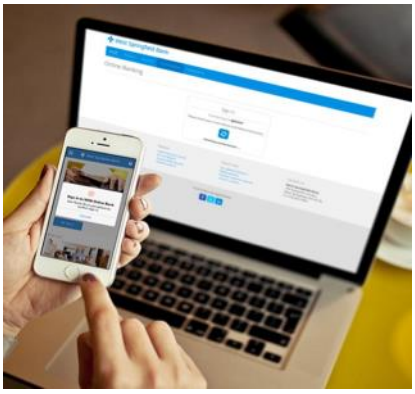
MFA: Multifactor Authentication. Requires a user to provide more than one form of identifying factor for identity verification and authentication purposes. In mobile-based MFA, the device becomes the factor that the user 'has', the PIN is something that the user 'knows'. A biometric can replace a PIN and is additionally something that the user 'has'.

SMD: Smart Mobile Device. A term coined by Goode Intelligence to denote a connected mobile device running a mobile Operating System. This includes Smartphones, Phablets and Tablets.

e-signature: An electronic signature, as defined by the European Union eSignature Directive is "data in electronic form which are attached to or logically associated with other electronic

The device is most commonly a smartphone: the Encap Smarter Authentication Platform harnesses the in-built capabilities of a person's smart mobile device to provide a context-aware authentication experience.

The smart mobile device becomes the central factor of multi-factor authentication enabled through Encap's device fingerprinting technology that uniquely and consistently identifies mobile devices. In its simplest implementation the user choses a PIN code that acts as the 'know' factor. The Encap platform's flexibility, based on the underlying device fingerprinting, extends to other technologies including biometric authentication – where supported by the device.



GPS and cellular network identification for determining location, touchscreen and accelerometer for behavioral biometric analytics and biometric sensors can all be used for convenient user authentication. For instance; If a bank customer owns an Apple iPhone that supports Touch ID fingerprint biometric authentication or Samsung's Fingerprint Sensor then Encap's platform can leverage Apple's in-built biometric system to enable its user to authenticate into their mobile app using their fingerprint.

Encap's Smarter Authentication Platform harnesses the in-built capabilities of smart mobile devices for strong authentication at scale but there are risks in using widely available consumer devices for high-risk uses.

Financial institutions and enterprises classify consumer smart mobile devices as 'untrusted' and 'hostile'. To combat this issue, Encap's authentication platform has the capability, through its ***App Defender*** feature, of detecting *jail-broken/rooted* devices and shielding against malware and tampering. If malware is detected on a device then that information can be transmitted to a risk engine managed by the service provider. Based on the service provider's risk profile, appropriate action can be taken for a particular authentication session; it could mean that the service provider does not want to accept the risk of a customer attempting to connect to their service from a malware-infested mobile device and reject the authentication request. Alternatively, the service provider may trust Encap's ability to protect its mobile app against

data and which serve as a method of authentication"

Risk Based Authentication (RBA): RBA is a non-static authentication method that is based on risk scoring to determine the identity of users.

Jailbreaking: Jailbreaking is the process of removing hardware restrictions on Apple iOS. Jailbreaking allows for root access to the iOS file system and manager. Jailbreaking is a security risk.

Rooting: Rooting is the equivalent of Jailbreaking for devices running Google's Android operating system.

malware and allow the customer to access their account.

PRODUCT EVALUATION

The **Goode Intelligence Product Evaluation Report** evaluates a product on a number of levels including ***Key Strengths***, ***Business Benefits***, ***Security Standards and Awards*** and ***Deployment Success***.

This report evaluates the ***Encap Security Smarter Authentication Platform***.

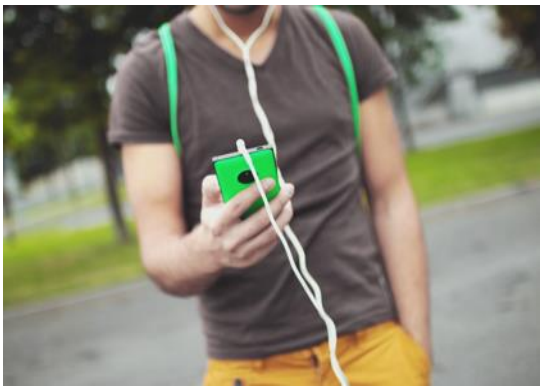
Key Strengths

Goode Intelligence has been covering mobile-based authentication since 2009 and has identified a number of key areas that an effective authentication solution should be strong in:

- Convenience & usability
- Security
- Scalable
- Omnichannel support
- Risk and policy based
- Context & process driven
- Support for multiple factors
- Simple to integrate into existing infrastructure
- Easy to provision & support for self-service lifecycle management

Convenience & Usability

The Encap solution offers a mixture of convenience and usability by being available on any smartphone or feature phone, and being a software technology it does not require specialist hardware or the availability of secure hardware environments on mobile devices.

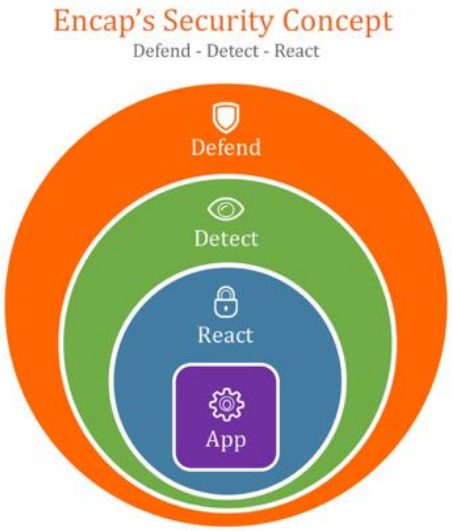


By supporting multiple devices per user and multiple users per device the platform meets the needs of today's multiple device users and the trend of sharing devices (especially tablets) amongst colleagues and family members.

Encap's client SDK allows financial services providers to embed flexible and strong authentication into their mobile apps providing customers the ability to actively choose the most appropriate authentication method.

The platform is being constantly updated to add new authentication methods as they become mature and in demand, allowing customers to benefit from the latest technology developments.

Security



Encap uses an authentication protocol that is built around an online Challenge–Response process that uses industry standard encryption and is based on a layered security model.

The authentication protocol is part of Encap's security concept, built around three security pillars; ***Defend***, ***Detect*** and ***React***.

Goode Intelligence believes that the blending of authentication and mobile security services is a unique feature for an authentication solution.

DEFEND

Defending ***data in use***, through its App Defender feature that detects malware and device tampering, ***data at rest***, through use of *Keychain* and encryption, and ***data in motion*** by utilizing application layer end-to-end encryption in addition to support for transport layer encryption like *TLS*.

DETECT

Encap detects a range of security threats to smart mobile devices including cloning, jailbreaking/rooting, debugging attempts, code

Keychain: A password management system developed by Apple.

TLS: Transport Layer Security is a cryptographic protocol that provides communications security over a computer network. It uses X.509 Certificates to encrypt data between two parties on a network.

injection, library injection and keylogging attempts.

While detection is important, it is not sufficient on its own. It is equally important to support organizations in reacting to security threats.

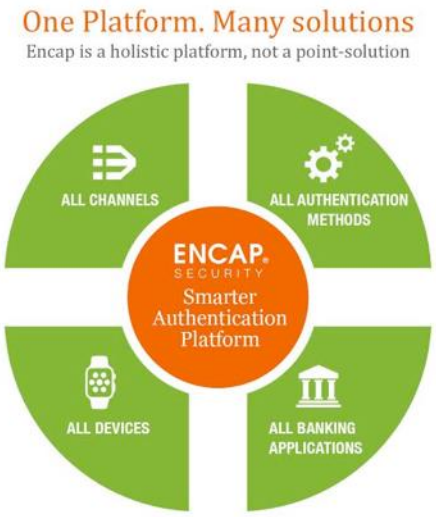
REACT

The product provides the necessary tools for organizations to react to security events that are raised by the authentication platform. By utilizing a policy-based approach to security events, organizations can either shutdown the authentication request (exit), lock access to the service or raise a flag for further investigation by security operations.

The rules that drive this function are configurable and aim to match business rules.

Scalable

Encap refers to internet scale versus enterprise scale for their authentication platform; the ability to scale to millions of users rather than thousands that are often seen for an enterprise deployment. This enables strong mobile-based authentication to be deployed to eCommerce users and to secure transactions in addition to supporting an internal work force.



Some mobile-based authentication solutions can also be limited to a particular piece of hardware or a specific device. Encap can scale to all devices as it is not dependent on secure hardware, specific mobile devices from a particular OEM or SIM-based solutions supplied by a particular mobile operator (or group of mobile operators).

Omnichannel Support

Encap Security's Smarter Authentication Platform supports omnichannel authentication including online, mobile, *IVR*, in-branch and via telephone call-centers; individually, in combination or all at the same time.

IVR: Interactive Voice Response is a telephone-based voice recognition system that allows people to interact with computers.

Risk & Policy Based

An agile and intelligent authentication solution needs to work in parallel with business rules. This includes being aligned with an organizations risk model.

Encap's authentication platform allows organizations to match business and risk rules to authentication sessions. This is managed through a feed that interfaces into an organizations existing risk management solution.

Context & Process Driven

Context and matching appropriate action to that context is key in authentication.

A combination of Encap's context engine and risk-based authentication allows organizations to match appropriate levels of authentication to specific transactions.

Context information can be applied to each transaction using information provided by the service provider as part of the authentication request. This can offer strong protection against *man-in-the-middle (MitM)* or *man-in-the-browser attacks (MitB)*.

MiTM: A Man in The Middle attack is where the attacker secretly relays and possibly alters the communication between two parties.

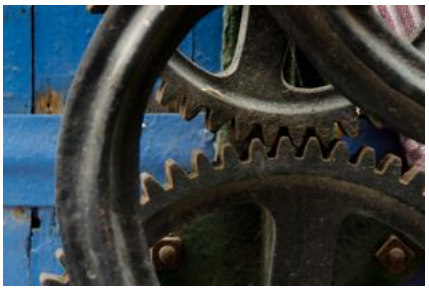
MiTB: A Man in the Browser attack is a proxy Trojan horse that infects a web browser to modify web page, transaction content or insert additional transactions.

Support for Multiple Factors

Linked to omnichannel support and context awareness is support for multiple factors. The latest authentication platforms need to embrace multi-factor authentication and Encap has been quick to support the latest convenience-driven authentication factors when they become available. Encap can vary and combine authentication factors based on the risk involved in each individual transaction.

This includes support for Apple Touch ID and Samsung fingerprint biometric authentication systems.

Simple to Integrate into Existing Infrastructure



The ability to 'drop-in' an authentication platform and quickly get users provisioned and connections made to existing services is critical.

Encap supports web services, through an API, and open authentication and authorization standards including *SAML* and *DSS*.

Encap has also successfully integrated its authentication platform to access managements systems from suppliers including Forgerock's Open AM and Ping Federation.

SAML: Security Assertion Markup Language is an XML-based open standard data format for exchanging authentication and authorization data between parties.

DSS: Digital Signature Standard based on the Digital Signature Algorithm (DSA).

Easy to Provision & Support for Self-Service Lifecycle Management

When you are dealing with hundreds of thousands – and possibly millions - of customers, an organization requires a solution that can be quickly and efficiently provisioned to end-users.

The Encap Smarter Authentication Platform allows users to enroll themselves in the system (if desired) and choose their preferred authentication method(s) based on selections made available by the service provider and available for their specific smart device. This allows for self-service identity management functions.

An administration interface is provided to ensure that the service provider can manage the full end-to-end lifecycle management. In addition, full administrative functions can be integrated into the identity management or business application through Encap's APIs.

Business Benefits

Goode Intelligence believes that the Encap Security Smarter Authentication Platform has a number of distinct business benefits that support banking omnichannel strategies and enable digital transformation projects.

The business benefits include:

- Increased take-up and adoption of banking services in most efficient banking channels
- Lower cost and higher security vs. other strong authentication platforms – includes no hardware costs as harnesses built-in smart mobile device capabilities
- Cost benefits – both in terms of opex and capex. Encap's Smarter Authentication Platform for a 500,000 user deployment would be 97.5 percent cheaper than a hardware-based OTP solution and 25 percent cheaper than a mobile-based soft token (OTP generated on the phone) solution.
- Designed for internet rather than enterprise scale – can support millions of users
- Allows for personalized and contextual access to digital services
- Not locked in to a single authentication factor – constantly adapts and built for the future
- Easy to customize and integrate with existing infrastructure including Identity and Access Management services
- Supports an omnichannel user experience – one device can become the authenticator for a range of digital channels
- The anti-malware and device security service allows for full eCommerce and banking services to be delivered to smart mobile devices – often these services are throttled as a result of weak authentication and endpoint security
- Ability to provide PKI-based eSignatures

Security Standards & Awards

The Encap Security Smarter Authentication Platform has been built in collaboration with financial institutions and regulators to meet strict global and national compliance standards.
Encap has been the recipient of multiple awards including the SC Magazine Awards 2015 & 2014 for Best Multifactor Solution.

Patents

Encap has 4 different patents that are at different stages of approval both in the US, Europe and other parts of the world. Two of Encap´s patents are granted in the US.

DEPLOYMENT SUCCESS

BinckBank – Dutch independent securities broker

BinckBank, an online bank for retail investors with a strong track record in offering mobile trading tools, completely renewed its mobile access recently. Already in 2010 BinckBank was the first bank in the Netherlands to facilitate trading by its apps for iPhone and Android. As customer centricity is a key element in BinckBanks' strategy, profound research among its users was the starting point for the development of the new mobile solutions. What mattered most to the customers was both safe and easy access to their investment portfolio so they could check their investment portfolio when and where ever they are. This required a simple and flexible login.

In search of a partner that could develop this solution, BinckBank chose Encap Security. One of the main reasons was that Encap provides both authentication and application security. Additionally the Encap authentication solution can also be reused across other digital channels that BinckBank offers to its customers. Currently the first phase of the Encap Solution is successfully implemented in the production environment. Jeffrey Severijn, Director ICT, BinckBank, confirms that the customers are very satisfied with the new mobile applications, the smooth user experience in particular.

BinckBank is an online bank for retail investors operating as market leader in the Netherlands and Belgium and expanding its business in France and Italy.

SUMMARY & RATING

Goode Intelligence defines a modern authentication solution to have the following characteristics.

Our evaluation of the Encap Security Smarter Authentication Platform concludes that the solution meets the requirements of a modern authentication platform and Goode Intelligence has awarded the product a **'Highly Commended'** rating (Goode Intelligence's top rating for Authentication and IAM). This rating has been awarded as the Smarter Authentication Platform is a highly customizable, adaptive and risk-based platform that meets the needs of highly-scalable connected digital services. It has the ability to be quickly integrated and rolled out to millions of end-users and is available for all smart mobile devices.

You can find out more about Encap's Smarter Authentication Platform on their website www.encapsecurity.com or access their Online Demo at www.encapsecurity.com/demo/.

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in information security including:

- Authentication and Identity
- Mobile Security
- Biometric Authentication and Identity
- Internet of Things Security

For more information on this or any other research please visit www.goodeintelligence.com.