THALES

nCIPHER PRODUCT LINE

Thales and VASCO Data Security help enable security and compliance in the gaming industry

VASCO
THE AUTHENTICATION COMPANY

The Thales and VASCO joint solution helps the online gaming industry secure gaming data and comply with regulations.

SOLUTIONS FOR:

- Comply with PCI DSS
- Protect gamers' identities and assets
- Verify and enforce age limits
- Safeguard online payments
- Ensure confidentiality of databases
- Satisfy audit requirements
- Stop fraud through backdating
- Does not affect the end user's experience

Online gaming requires more security

The gaming industry has always had to protect against fraud. Now it is also becoming the subject of more and more legislations to protect gaming companies, gamers, financial institutions and taxpayers. Various local regulations require that gaming transactions can be audited. The global Payment Card Industry Data Security Standard (PCI DSS) requires that gamers' credit card details are kept secure. Gamers are expecting that the gaming industry protects their identities and assets. Gaming companies need to be able to demonstrate that their systems are secure and trustworthy, otherwise a data breach or fraud case may cause gamers to take their business elsewhere.

Protecting gamers' identities and assets

Gamers often spend a lot of time and money to build their online identity, making it a valuable asset that must be protected. Even if a game does not pay out real money, virtual assets in multi-player online games can often be sold for hard cash. Heavy users and high rollers increasingly expect gaming companies to protect their identities and therefore their assets.

Thales and VASCO offer a joint solution that ensures gamers' identities are protected by using strong, dynamic passwords. The combination of dynamic passwords generated by DIGIPASS authentication device (something you have), and a username or PIN (something you know) is also referred to as strong authentication. This technique is used to protect against identity theft and provides passwords that change every 32 seconds and can only be used once. A wide range of authentication devices exist: single button devices, USB devices, PIN pad devices, smart card readers, and even authentication software for mobile phones.

Verifying and enforcing age limits

Enforcing age limits of online players is much harder in the online world than in brick-and-mortar arcades and casinos. Gaming companies often either have to enforce age limits by law or do so voluntarily to preempt harsh legislation or potential legal battles.

Thales and VASCO offer an integrated solution that covers the full lifecycle management of user credentials and authentication devices. This includes the enrollment process required for age verification as well as issuing authentication devices. This ensures that the enrolled user's identity cannot be easily passed on or stolen, demonstrating that the gaming company is exercising due care in limiting its games to individuals who pass the legal age requirements. Identity vetting can be performed with local organizations.

Protecting credit card data

Because most online gaming companies accept credit or debit cards, they must comply with the Payment Card Industry Data Security Standard (PCI DSS). The standard states that credit card information must never be unprotected when transmitted over public networks or stored on electronic media.

Safeguarding online payments

The joint Thales and VASCO solution can protect payment details as they flow through the gaming systems. Gamers typically enter their credit card information in a browser that protects the connection between the browser and the server through the SSL (Secure Socket Layer) protocol, the same technology that protects online banking customers around the world. Thales and VASCO can help protect SSL keys with hardware security to ensure that encryption keys are stored in the fewest possible locations and forms (as required by PCI DSS). This also adds internal controls such as separation of duties and multiple-person controls to ensure that a potential rogue administrator cannot defraud the system.

Past breaches have shown that web servers are often the weak point exposing credit card data because they have either been hacked, are vulnerable to insider attacks, or have been infected with malicious software. The joint Thales and VASCO solution helps ensure credit card data, PINs and passwords that are protected by SSL are never exposed on the web server and only processed inside hardware security modules. Credit card information can be re-encrypted to be stored in a database or sent to a payments processor. This approach protects against rogue administrators and Trojan attacks.

Ensuring confidentiality of databases

Databases are full of confidential information, such as gamers' personal information, credit card data, and financial transactions. PCI DSS requires that credit card information must not be stored unencrypted.

The joint Thales and VASCO solution leverages Transparent Data Encryption (TDE), the native encryption functions of Oracle and Microsoft databases, and adds several operational, compliance and security benefits to its key management. It reduces the cost of operations for large database farms in mixed environments, introduces additional internal controls, and enhances overall security.

Satisfying audit requirements

Because changing electronic information is very easy and manipulations hard to spot, auditors often require the use of digital signatures to prove the identity of the author, authenticity of the content, and ensure the non-repudiation of transactions.

The joint Thales and VASCO solution can digitally sign financial and gaming transaction logs with tamper-responsive security hardware to ensure that data cannot be manipulated without detection.

Stopping fraud through back-dating

Many games, such as roulette, horse races and lotteries, are based on the gamer guessing the outcome of a future event. Because it's much easier to "guess" the winning horse after the race is over, it's critical that online gaming companies can verify that a bet has been entered before the race.

The joint Thales and VASCO solution can help prevent fraud through back-dating by adding secure auditable time stamps to electronic data such as gaming transactions and betting slips.

About Thales

Thales is a global technology leader for the Aerospace, Space, Defence, Security and Transportation markets. In 2008, the company generated revenues of 12.7 billion Euros with 68,000 employees in 50 countries. With its 25,000 engineers and researchers, Thales has a unique capability to design, develop and deploy equipment, systems and services that meet the most complex security requirements. Thales has an exceptional international footprint, with operations around the world working with customers as local partners.

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security serving customers in more than 100 countries, including several international financial institutions. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

Americas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Australia: Level 2, 103-105 Northbourne Avenue, Turner, ACT 2601, Australia • Tel: +61 2 6120 5186 • Fax: +61 2 6120 5101 • E-mail: sales.australasia@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com