BOMcheck Information Security Policy

BOMcheck is designed and implemented to achieve the highest commercial data security standards. All sensitive data on BOMcheck is stored securely by encrypting the data to PCI DSS standards. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Administrator access to the BOMcheck system is restricted to only three security-approved BOMcheck staff and BOMcheck's contract with each Member includes strict obligations on BOMcheck to ensure security and confidentiality of the Members' data. The security of the data on BOMcheck is tested every day by McAfee who use thousands of different hacking techniques to attack the www.BOMcheck.net web database system. BOMcheck web application security is assessed during an annual 5 day audit by the Siemens Cyber Emergency Readiness Team. The BOMcheck web database system is hosted using the same internet server arrangements as www.amazon.com.

1 Contractual obligations and Administrator access restrictions at BOMcheck

Administrator access to the BOMcheck system is restricted to only three security-approved BOMcheck staff. These named individuals have received appropriate security training. BOMcheck Steering Group companies do not have any special access to the BOMcheck system.

BOMcheck's contract[1] with each Supplier Member includes strict obligations on BOMcheck to ensure security and confidentiality of the Supplier Members' data, including the following clauses:

5.7 *BOMcheck will not use any other means to distribute the Member's Data except via the Database. BOMcheck will not provide the Member's Data to any party who has not signed a Manufacturer's Agreement to use the Database. BOMcheck will not in any way sell, transfer, (sub-) license or otherwise commercially exploit the Data provided into the Database.*

5.8 *BOMcheck will treat any Data in the Database as strictly confidential and will not access the Member's account unless instructed to do so by the Member. Exception to this is system statistics calculation such as e.g. number of Regulatory Compliance Declarations, number of Full Materials Declarations etc. Furthermore BOMcheck's internal access to Data is restricted to specially selected persons that may need access under supervision of security personnel for system maintenance purposes*

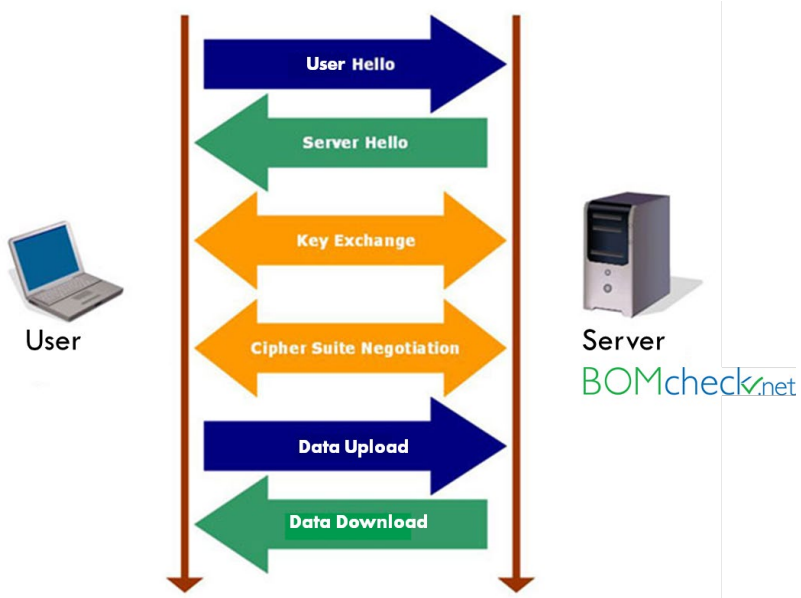
2 TLS 1.2 (SSL 1.3) security encryption of all communication between BOMcheck and the company's internet server

BOMcheck uses the TLS 1.2 (SSL 1.3) encryption protocol to prevent any eavesdropping or tampering of data which a company transmits to www.BOMcheck.net and data which a company receives from www.BOMcheck.net, Figure 1.

As part of the TLS 1.2 (SSL 1.3) encryption protocol, BOMcheck encrypts the segments of network connections above the Transport Layer, using asymmetric cryptography for privacy and a keyed message authentication code for message reliability. When a user logs into BOMcheck, the BOMcheck system communicates with the user's internet server to establish the parameters that will be used to ensure the highest level of security for the connection. BOMcheck chooses the strongest cipher and hash function that the user's server is able to support and then uses this for all communications. BOMcheck then sends our digital certificate to the user's server which includes the trusted certificate authority (CA) and BOMcheck's public encryption key. The user's internet server may contact the trusted certificate authority (CA) server and confirm the validity of the BOMcheck public encryption key before continuing.

[1] The BOMcheck Supplier Member Rules are published at https://www.bomcheck.net/suppliers/member-rules

Figure 1. TLS 1.2 (SSL 1.3) security encryption of all data to/from https://www.bomcheck.net

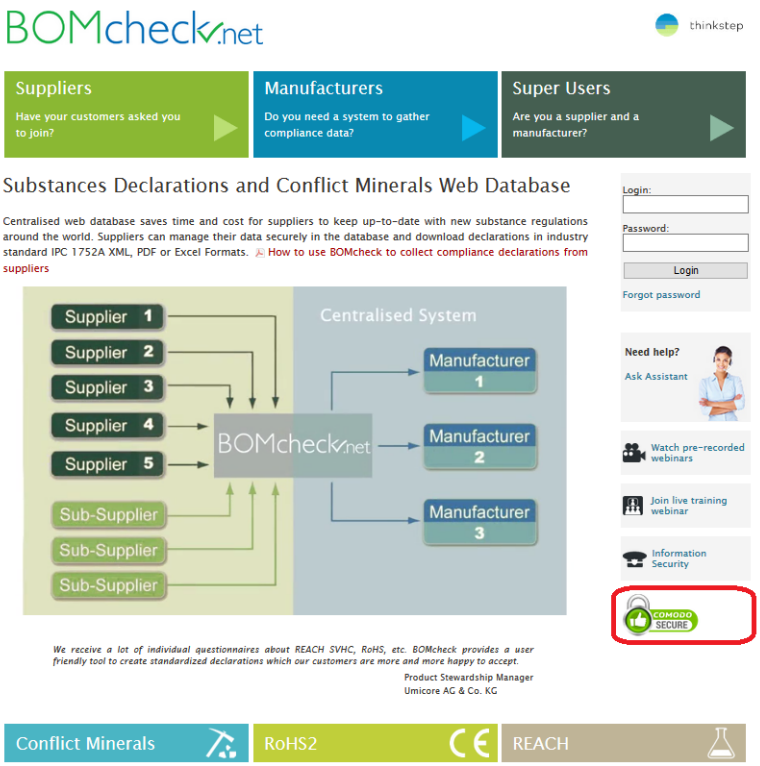


In order to generate the session keys used for the secure connection, the user's server then encrypts a random number with the BOMcheck public encryption key and sends the result to www.BOMcheck.net. Only www.BOMcheck.net can decrypt this message using BOMcheck's private key. This concludes the security handshake between BOMcheck and the user's server and begins the secured connection. This random number is then used to encrypt and decrypt all data that a user transmits to www.BOMcheck.net and all data which a user receives from www.BOMcheck.net. If any one of the above steps fails, the TLS handshake fails and the connection is not created.

3 Comodo Trusted Site Seal

The BOMcheck web database system is certified to the Comodo Trusted Site Seal which confirms that all data entered into BOMcheck is securely encrypted, Figure 2. BOMcheck utilises Extended Validation SSL Certificates which provide stronger security and combat phishing attacks.

Figure 2. Comodo Trusted Site Seal Certification



4 BOMcheck web application security is audited by the Siemens Cyber Emergency Readiness Team.

SIEMENS

BOMcheck web application security is assessed during a 5 day audit each year by the Siemens Cyber Emergency Readiness Team (CERT).

The web application security assessment of BOMcheck has been performed to the best knowledge of Siemens CERT, which is based on state-of-the-art know-how and many years of experience. Siemens CERT is determined to identify all security vulnerabilities within the scope of the assessment. However, due to the inherent nature of security assessments and the limited timeframe, it is impossible to guarantee that no vulnerability will remain undetected.

5 BOMcheck uses the same internet server arrangements as www.amazon.com

amazon web services™

BOMcheck is hosted on servers which are provided by Amazon Web Services (AWS). AWS customers include Amazon, Ericsson, Hitachi, Virgin Atlantic, European Space Agency, US Department of State.

AWS is compliant to several security certifications and third-party audit programs including:

- **SAS70 Type II.** The report covers the detailed controls that AWS operates along with an independent auditor opinion about the effective operation of those controls.
- **PCI DSS Level 1.** AWS has been independently validated to comply with the PCI Data Security Standard as a shared host service provider.
- **ISO 27001.** AWS has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering infrastructure, data centers, and services.
- **FISMA.** AWS enables government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). AWS has been awarded an approval to operate at the FISMA-Low level. It has also completed the control implementation and successfully passed the independent security testing and evaluation required to operate at the FISMA-Moderate level. AWS is currently pursuing an approval to operate at the FISMA-Moderate level from government agencies.

AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely.

Further details about AWS security systems are available at:
http://aws.amazon.com/security/
http://aws.amazon.com/about-aws/whats-new/2009/11/11/aws-completes-sas70-type-ii-audit/