Brock University

IT ENCRYPTION STANDARDS

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy.

The purpose of this document is to support and outline in detail the requirements of the IT End User Communication and Encryption Policy. These requirements are mandatory and must be adhered to by all employees, students, consultants, vendors, IT System administrators and application developers.

This document outlines requirements that must be adhered to for encryption to be used and the deployment standards for each type of encryption.

SCOPE

This document is intended for all employees, students, consultants, vendors, IT System administrators and application developers.

REQUIREMENTS

Web Server Traffic

Any time a web application is accessible via public networks and contains sensitive data, communications with that web server must be done via a secure connection (HTTPS) which has been encrypted using public key encryption.

Password Authentication

Any communications which include usernames and passwords must use a secure communication channel or be encrypted.

Public Key Encryption Certificates

All public key encryption certificates used for public and internal communication services must be verified and approved by the ITS Infrastructure team.

A wildcard certificate that can be used to secure any *.brocku.ca domain must be purchased and maintained by the Information Technology Services (“ITS”) Infrastructure team.

Use of public key encryption certificates must adhere to the following:

1. The private key must only be stored in a primary location and a backup location. In each case this private key must only be accessible by authorized system administrators and the application which needs the key to function.
2. When a system uses the wildcard certificate maintained by ITS, a unique key must be generated and used to create a unique wildcard certificate for that system.
3. Individual certificates must be purchased for services and situations where the wildcard certificate cannot be used. These certificates belong to and will be managed by the ITS Infrastructure team.
4. All certificates purchased must be from an ITS-approved Commercial Certificate Authority.
5. Self-signed or enterprise certificates must not be used for any publicly accessible services.
6. Enterprise certificates must be used for internally managed services such as Active Directory. These certificates belong to and will be managed by the ITS Infrastructure team.

Data Encryption Keys

Keys used to encrypt other keys must be stored separately from data encrypting keys.

Keys used to encrypt other keys must be at least as strong as the data encrypting keys they protect.

RESPONSIBILITIES

System Administrators

System administrators are required to implement the appropriate encryption methods where necessary and deemed required by data owners. This is usually identified as part of the project management implementation framework.

Credit card data must not be stored in any Brock University managed system. System administrators must enforce this during discussions with data owners.

System administrators with access to public key encryption certificates and keys or passwords are responsible for ensuring secure storage of the keys and passwords. This includes ensuring that keys and passwords are not stored in locations which are unnecessary for the operation of the application. A backup storage location is permitted for the purposes of disaster recovery in the event of system failure.

Infrastructure Services, ITS

Infrastructure Services, ITS is responsible for acquiring and maintaining all public key encryption certificates.

Infrastructure Services, ITS is also responsible for creating and maintaining any certificate authorities and enterprise certificates required for local infrastructure use such as Active Directory.

DEFINITIONS

Commercial Certificate Authority

Commercial CAs charge to issue certificates, and their customers expect the CA's certificate to be included by most web browsers, so that secure connections to the certified server work smoothly out of the box

Enterprise Certificate

A public key certificate which has been generated using a local certificate authority and is used for securing local infrastructure. Although technically a self-signed certificate, an enterprise certificate is created, managed and secured using ITS-managed resources

Protected Network

A section of the Brock University network which is not accessible to computers/ devices which have either not been granted authenticated network access or have specifically been connected by ITS

Public Key Encryption

A class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret and one of which is public. Although different, the two parts of this key pair are mathematically linked

Public Network

Any network which is accessible to having communications intercepted by unauthorized devices or computers. This would include, but is not limited to, the public internet, wireless networks, and computers/devices not within the University’s protected networks

Secure Communication Channel Any communication method between one or more computers where the data is encrypted during transmission so that the data cannot be viewed by anyone except the intended recipient

Self-signed Certificate A public key certificate which has been generated and signed locally instead of a public certificate authority