Policy on Securing Electronic Communications Using SSL

Document summary

Effective date	2017-05-26	**Last updated**	2017-05-26
Document owner	Enterprise Infrastructure Services: Information and Cyber Security Team: UCT - CSIRT		
Approved by	UICTC	**Reviewed by**	UICTC
Enquiries	Enterprise Infrastructure Services: Information and Cyber Security Team, CSIRT: csirt@uct.ac.za		

Purpose

The purpose of this policy is to ensure university-wide appropriate use and implementation of SSL certificates and associated technologies, which are used to confirm identity, secure communications between parties, and ensure integrity of transmissions.

Definitions

Term	Definition
Certificate Authority (CA)	An authority in a network that issues and manages security credentials for message encryption.
Certificate, also Digital Certificate:	An electronic document used to bind together a public key with an identity.
SSL/TLS, also Secure Socket Layer and Transport Layer Security	Protocols used to authenticate servers and clients and to encrypt messages between the authenticated parties
Wildcard Certificate	Allows you to secure multiple sub domains on one domain on the same server using *.domain.com pattern for the common name.

Applicable to

All systems hosting UCT Electronic Information and/or data, irrespective of owner or location.

Exclusions

The use of SSL certificates for data at-rest is not a requirement, except where specifically mandated. The certificate standards as set out below, apply in all cases where applied.

Policy summary

Any University system, application, appliance or site is required to secure and protect the following types of information when:

- Authentication of some or all users who visit the site is required (e.g., usernames and passwords are used for access);
- Visitors need to have the option of verifying that they are connected to the correct ("official") web site;
- Confidential institutional information is displayed;
- Personal information is viewed and/or submitted by visitors to the site, or via electronic transactions;
- Integrity of the information presented or entered is important (i.e. an assurance that nothing can be changed in transit/transmission);
- Financial or electronic commerce transactions are executed (i.e. credit cards are accepted for payments); and
- Updates (adds, changes, deletes) are being made to institutional information.

This is achieved by the correct use of SSL certificates, which need to be adequately, correctly and appropriately managed (created, applied, stored and validated) throughout their lifecycle.

Policy details

This section outlines the acceptable use of SSL certificates at UCT. Additional strength, configuration, and validity requirements are included in Appendix A. Certificate Authority requirements are included in Appendix B. Requests for SSL certificates that do not meet these requirements may be denied or subject to revocation. Application or vendor requirements shall not result in a reduction of the minimum requirements stated in this policy.

1. A. Wildcard SSL Certificates

Only ICTS units may own or manage a wildcard cert for the *.uct.ac.za domain. Faculties and departments may obtain wildcard certificates for their sub-domain(s) and servers only (e.g. *.mydomain.uct.ac.za). These may not be applied to UCT centrally provided hosts. See below for additional details.

Unless specifically disallowed above, wildcard SSL certificates may be appropriate for a single server with more than one host sharing a single IP address.

UCT does not permit wildcard certificates for systems handling confidential or personal data.

2. Self-Signed SSL Certificates

Self-signed SSL certificates are only allowed when *all* the following apply:

- All clients can have the certificate manually installed;
- Installation is on development and test systems only; users should be advised that a self-signed certificate is in use and provided with sufficient information to know how to respond to certificate errors or warnings; and
- The private key is password protected.

Self-signed SSL certificates are not allowed in the following circumstances:

- When data on the server is accessible by the public or via a public IP;
- On a production service deployed to a wide number of users; and

- When confidential or personal data is involved.

3. Private Key Management

Private keys must be protected to same degree as required for the data the key is protecting. Protecting the device storing the private key is sufficient to meet this requirement.

Where passwords are used to protect private keys, those passwords must comply with the campus Password Policy and Password Strength and Security Standards. Passwords are strongly recommended for private keys protecting confidential and personal data.

Systems are not permitted to operate with expired certificates.

Where SSL certificates are shared or span across multiple hosts, the security requirements of the most sensitive member host prevails.

Exceptions to the remediation (whether in principle or with regards to the timeline stipulated), will be escalated to the EDICT for approval, and will be recorded for the attention of UICTC, UCT Risk Committee and the UCT Information and Cybersecurity Governance Committee.

Policy violations

Violations of these guidelines may be dealt with in accordance with UCT procedures established for staff and/or student discipline. In addition, non-conformance with the policy may result in the disconnection of a computing device from the UCT network.

Roles and responsibilities

Role	Responsibilities
System Administrators	Generate CSR's and install or remove certificates
UCT CSIRT team	Provides infrastructure for periodic scanning and validation of SSL certificates Provides information and best practice guidance, including disseminating security alerts and advisories
ICTS – TSS	Provides assistance to system administrators

Related links

- UCT Account and Password Policy
- UCT CSIRT Process and Plan
- Qualys SSL Labs "SSL/TLS Deployment Best Practices"
- WebTrust Principles and criteria

Appendices

A. **Server Certificate and Related Configuration Requirements**

An exception is required if an implementation cannot meet these standards. Compensating controls may be required if an exception is granted.

Implementations must meet Qualys SSL Labs "SSL/TLS Deployment Best Practices" described at https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices Note: The TENET certificate service meets the CA requirements outlined in these Best Practices.

Servers that achieve a "Grade A" or higher rating on the Qualys SSL Labs Server Test at https://www.ssllabs.com/ssltest/analyze.html are considered to meet these Best Practices.

IMPORTANT: Always check: "Do not show the results on the boards" when running the SSL Labs Server Test so results are not posted publicly.

- Re-validation/re-testing should be done at least annually.
- Significant findings from UCT CSIRT security scans must be addressed.

Certificate Renewal:

- Keys must be regenerated and certificates re-signed when renewing a certificate.
- Annual renewal is required for systems handling restricted data.

Certificates for systems that do not handle restricted data must be renewed after no longer than three years. It is recommended that all certificates be renewed annually.

B. **Certificate Authorities (CA) must meet the following requirements**:

CA can provide the following support through life of the certificate:

- The ability to revoke a certificate
- Retain the Certificate Signing Request (CSR) and ability to reissue the certificate
- Maintain a list of UCT contacts authorized to administer or manage the certificate
- Provide renewal notices
- CA root and intermediate certificates are recognized by ICTS supported browsers and desktops
- CA verifies the applicant's credentials (e.g., requester is affiliated with UCT)