

At Teranet, the security of our systems is our number one priority. As of April 2005, over 9 million online transactions have been completed using our Teraview® and WritFiling™ remote access services. Not one of those transactions is known to have been done by someone who has gained fraudulent access to the system, either by identity theft, such as obtaining someone else's access keys, or by tampering with data submitted by legitimate users.

The Teranet security service, called Portas®, secures access to our systems. Portas service includes Public Key Infrastructure (PKI) and Certificate Authority (CA) infrastructure and utilizes Entrust Authority™ products. PKI technology is a well-established technology for managing the digital identities used for authenticating users and ensuring the security of transactions.

We regularly examine our systems to ensure that our processes, infrastructure and technology remain world class and continue to exceed industry standards for the security and reliability of our records.

### The Five Elements of Teranet's Security

The foundation of Teranet's security relies on five elements:

- Authentication – You are who you say you are.
- Authorization – You are allowed to access specific data or functions.
- Digital Signatures – You did that transaction (non-repudiation) and the transaction data has not changed (integrity).
- Encryption – Your data is private and confidential.
- Security Management – Your security is managed effectively and efficiently.

### Securing Access: The Process for Becoming a User

All users who wish to access our Teraview or WritFiling systems are required to have a Portas PKI credential. Even a title search in the Teraview system, with no records being changed, requires this high level of security.

The application process for a PKI credential is rigorous and requires face-to-face verification of an applicant's identity. Applicants must:

- provide personal and challenge question information;
- produce two forms of approved identification, such as a passport, birth certificate or driver's licence, at least one of which must be photo identification;
- have their identity validated by a lawyer (other than the applicant), a Notary Public, a designated Province of Ontario Land Registry Office representative or a designated Teranet representative; and
- have their signature witnessed by the same validator.

When a lawyer is applying for a PKI credential, we use the Law Society of Upper Canada's database to verify that the lawyer is in good standing as at a certain time. The record of each lawyer in the Portas CA is compared against the Law Society's database on an ongoing basis to ensure that only lawyers in good standing can continue to access the Teraview and WritFiling systems.

Once an application is approved, the applicant must contact us personally to activate their credential. A Teranet representative then returns the call using contact information on their application and engages in a process of confirming the identity of the individual on the phone based on information contained in the application.

At the end of this verification process, a physical medium, such as a diskette or USB storage device is

---

loaded with encrypted identification information. This credential must be used along with the user's secret and confidential passphrase to access to the system.

The credential is similar to a bank card: without the username/secret passphrase, a lost or stolen diskette is useless, just as the username/password is useless without the diskette. Stringent rules govern the format of the secret pass phrase and users are compelled through system controls to change it frequently.

Lost or stolen credentials are immediately disabled as soon as Teranet is notified. Before we will provide a user with a new credential, the user must go through a rigorous process to verify the user's identity.

Teranet has also worked closely with the Law Society of Upper Canada regarding the use of a PKI credential and the importance of maintaining its integrity. The Law Society's Rules of Professional Conduct deal specifically with the professional obligations of lawyers to protect their credentials and secret pass phrases, and ensure their staff do the same and Teranet has terms and conditions that provide restrictions on the use of these credentials.

#### Additional Controls Ensure Security

PKI technology is the foundation of Teranet's approach to security. But PKI alone is not the whole story. We have worked (and continue to work) with the Ontario government, the Law Society and security experts to include system design components and internal processes to provide additional levels of security.

- Teraview, WritFiling and Portas systems include comprehensive logging of events and provide a solid audit trail. Unlike signatures on a paper document, any electronic signatures on a changed document can be irrefutably traced back to a specific user's credential, and automated tools are available to monitor and identify suspicious or unusual activity. This capability to quickly and reliably identify fraudsters is, in itself, a deterrent to potential fraudulent activity.
- Teranet staff, including Customer Service staff, who have access to the Portas processes and who verify user identities are subject to background checks. Teranet's Security Operations Group, who oversees all aspects of Teranet's security, keeps their knowledge and expertise current through active participation in industry events, committees and advisory panels.
- Teraview is a sophisticated system designed for use by regular, professional users. In order for a user to complete any change to a document, he or she must be familiar with the exact process and complete the requisite steps correctly. Users must also establish a special bank account for use with the Teraview system. This makes it more difficult for an untrained user who has fraudulently gained access to the system to successfully submit a changed document.
- If a document awaiting registration is amended or changed after it has been digitally signed, the digital signatures are automatically removed and both parties to the transaction must re-sign the document. This prevents a document from being altered without a signatory's knowledge. As well, all signed in-progress documents have to be re-signed if a signing key has been recovered.
- When a title record is changed through the online system, it is submitted for scrutiny by Ontario government officials. It must be reviewed and the content of the document confirmed by the government's Land Registry staff before it receives certification.

#### Teranet: A Leader in Secure Access

Teranet itself has earned the difficult-to-obtain TruSecure® certification. TruSecure certification is awarded only after extensive auditing and review of an organization's business processes, systems and environment and is subject to ongoing auditing and review by TruSecure.

Teranet is a leader in providing secure access to vital government and legal documents. Our track record proves it: since 1999, our users have successfully, securely completed over 4.4 million electronic registrations.

#### Technical Background — Why is “Powered by Portas” Secure?

A Public Key Infrastructure (PKI) is a collection of tools, processes, policies and other components, including a Certificate Authority (CA) and a Registration Authority (RA) to authenticate the identity of users. The following section provides more in-depth information on PKI in general, including the key CA and RA components, and on Teranet’s Portas security services.

#### What is PKI?

The purpose of PKI is to manage keys and certificates so that an organization can establish and maintain a trustworthy networking environment. The Portas® service utilizes Entrust® components, which enable the use of encryption and digital signature services across different applications within Teranet.

For public-key cryptography to be valuable, users must be assured that the other parties with whom they communicate are “safe” – that is, their identities and keys are valid and trustworthy. To provide this assurance, all users of a PKI must have a registered identity. These identities are stored in a digital format known as a public key certificate.

#### What are a Certificate Authority and a Registration Authority?

Teranet has been a trusted Certificate Authority (CA) and Registration Authority (RA) since 1999.

The CA comprises the people, processes, and tools to create digital certificates that securely bind the names of users to their public keys. In creating certificates, the CA acts as an agent of trust. The RA supports the administration of a CA by instituting operational and technical controls, establishing procedures for providing certificates, creating policies and providing authentication and certification services to clients

The CA creates certificates for users by digitally signing a set of data that includes:

- The user’s name in the format of a distinguished name (DN). The DN is unique and specifies the user’s name and any additional attributes required to uniquely identify the user.
- A public key of the user. The public key is required so that others can encrypt data for the user or verify the user’s digital signature
- The validity period of a certificate. In Teranet we have set a security policy to run a regular check on all inactive users (un-used certificates).
- The specific operations for which the public key is to be used. Teranet makes use of the keys for digital signatures for the land registration and writs of execution systems.

The CA’s signature on the certificates permits easy detection of any tampering. Since the integrity of a certificate can be determined by verifying the CA’s signature, certificates are inherently secure and can be distributed via a publicly accessible directory system. Users can trust that the certificate and its associated public key belong to the entity specified by the DN. Users also know that the public key is still within the defined validity period.

Teranet uses the Entrust Authority Security Manager for its CA system to enable the use of digital signatures, encryption and permissions management services across Teranet applications. Specifically, it

- securely stores the CA private keys;

- issues certificates on a per-user basis, providing user-specific privilege and access control information in a user's certificate;
- publishes a user certificate revocation list (CRLs), including expiry time and issuance frequency, to allow verifiable communications;
- maintains an auditable database of users' private key histories for recovery purposes in the event that users lose access to their keys; and
- supports standard based certificate (x.509), revocation system (CRL, OCSP), directory communication (LDAP), application to CA communication (PKIX, PKCS), hardware support (PKCS), broad algorithm support, as well as standards-based cross-certification (PKIX and PKCS) and policy constraints (X.509v3 constraints).

### Certificate Policy and Certificate Practice Statement

Every CA must have a Certificate Policy (CP) and a Certificate Practice Statement (CPS). The CP states the policies that govern the CA, including requirements for issuing certificates and which applications can be used with the certificates it issues.

The CPS details the practices in place to carry out the policy defined by the CP. It mandates such points as subscriber application workflow practices, employee training, CA server security policy and encryption levels for each certificate assurance level. The Portas CPS is highly detailed and well structured. A thorough and current CP and CPS, such as those for Portas, are essential for a well-managed, secure CA. Any proposed changes must be scrutinized to ensure that security is in no way compromised. Teranet's CP and CPS are managed by a committee of legal, security and operations experts and senior officers of Teranet, who must approve all changes.

### What is Two-Factor Authentication (Token-based)?

Two-factor authentication means that a user must have more than a password to gain access. The two factors are:

- Something you have: In the Teranet system, this is a physical credential (a floppy diskette or a USB storage device) that stores a user's unique Entrust profile (.epf files). This data is encrypted.
- Something you know: This is a pass phrase created by the user according to stringent rules governing its format that prevent users from selecting "easy to guess" passwords. The system forces users to change their passwords on a regular basis.

Before users can log in or carry out certain activities, they must present both their physical credential and their associated username/pass phrase.

### Assurance Levels

There are 4 classes of assurance levels as defined by the Government of Canada: Rudimentary, Basic, Medium and High.

Teranet is currently issuing Medium Level assurance certificates with some additional standards from the High Level assurance definition. Medium Level is a high level of security and is the second highest assurance level available. No other land registration and legal filing system in Canada operates at such a high level of assurance. Due to its complexity, cost and implications for a user's personal privacy, High Level assurance is rarely implemented and is normally used only for issues of military and national security.