February 2013

End to End Trust

Key Points

- End to End Trust is a vision for enabling safer, more trusted computing experiences through broad industry and government collaboration.
- The core concepts of End to End Trust include embracing security and privacy fundamentals; building a trusted stack that spans hardware, software, data, and people; aligning technical, social, political, and economic forces; and creating a claims-based identity meta-system.
- Microsoft is currently working with policymakers, industry partners, and advocates on several important initiatives that include increasing the level of assurance of identity information through in-person proofing, discovering ways to assess the health of devices to help reduce risk, enabling policy-based access control to help protect data as it moves around the Internet, and developing appropriate privacy protections to help users control the disclosure of their data.

BACKGROUND

The Internet allows people to use tools that enrich lives, build commerce, and facilitate communication around the globe. But the more people connect online, the greater the need to understand the implications of security, safety, and privacy on the Internet. Microsoft's Trustworthy Computing and the vision of End to End Trust help provide context for policymakers worldwide who are working to develop cyber security policies and initiatives while balancing the need to safeguard individual privacy.

Microsoft is committed to sharing insight and guidance with decision makers and public policy leaders to help define priorities and take substantive action to ensure secure online practices.

The core concepts of End to End Trust are these:

- **Security and privacy fundamentals**. A trusted online environment relies on technology built from the ground up with security and privacy in mind.
- **Technology innovations**. End to End trust requires an environment in which reasonable and effective trust decisions can be made. This environment depends on a trusted stack—security built into the hardware, trusted software, trusted data, and trusted people.
- **Social, economic, political, and IT alignment**. Technical solutions to implement the End to End Trust vision may fail if there aren't suitable economic models to support them. Solutions could also trigger a backlash if they fail to take into account existing social norms such as privacy. Working together to align technical, economic, political, and social forces greatly increases the ability to make progress.

Microsoft is currently engaged in three key projects with government and industry partners to realize this vision:

- **Verified identity**. High-value transactions, such as online banking, demand a high level of assurance. One way to increase the level of assurance of identity information is to perform in-person proofing. Because many online transactions do not need high levels of assurance, establishing an online identity system that can provide a range of assurance levels is essential. It is also important to build in privacy protections—for example, it may not be

necessary to know a person's name. Such a system would support new identity services that would verify claims about people and devices. Microsoft is helping others create such a claims-based identity system.

- **Device health**. There's a great need for a simple, consistent, and secure way to measure and independently verify the trustworthiness of devices that connect to the Internet. The goal of the device health project is to create a standards-based solution to verify computing devices that are used for high value transactions.
- **Policy-based data protection**. One of the biggest challenges on the Internet (and in the cloud) is ensuring that sensitive data can be accessed only by those who are authorized to do so. Sensitive data is often shared outside organizations as well as on a wide variety of devices. This project centers on creating solutions that strongly tie data and its access policy together so that no matter where the data ends up, the policy will be honored.

MICROSOFT APPROACH

Microsoft has published the following guidance to help further security and privacy fundamentals:

- The Security Development Lifecycle is a security-assurance process that has been shown to reduce the number and severity of vulnerabilities in software.
- Privacy Guidelines for Developing Software Products and Services offers best practices for developers.

Microsoft technology innovations enhance security:

- Microsoft Security Essentials is a free consumer antimalware solution for Windows XP SP2, Windows Vista, Windows 7, Windows 8, and Windows RT.
- Microsoft Forefront is an integrated portfolio of protection, identity, and access products for organizations both on premises and in the cloud.
- The Microsoft identity and access solution allows organizations to establish and easily maintain a single, consistent representation of identity across the datacenter and cloud. The Information Protection solution automatically discovers, protects, and manages confidential information throughout an organization by integrating with existing platforms and apps.

POLICY CONSIDERATIONS

- Microsoft continues to engage with governments as a trusted advisor, to enhance the security, privacy, and reliability of the cyber ecosystem, and to defend against cyber threats. The company believes that collaboration within industry and with governments through strategic partnerships and outcome-focused initiatives are critical to that mission.
- Microsoft has joined with industry partners to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address online crime.
- Microsoft supports government funding of basic security research to help improve the security of online systems.

Helpful Resources

Microsoft's End to End Trust
www.endtoendtrust.org

Security Development Lifecycle
www.microsoft.com/SDL

Privacy Guidelines for Developing Software Products
aka.ms/privacy-guidelines