

News Release

FOR IMMEDIATE RELEASE

Entrust EAC ePassport PKI Operates 'Flawlessly' at Prague, Leveraging Slovenia and UK Infrastructure
Entrust demonstrates perfect PKI certificate exchange for EAC interoperability test across multiple countries and vendors

DALLAS — September 18, 2008— At a key interoperability test for second-generation ePassports in Prague last week, Entrust, Inc. (NASDAQ: ENTU) demonstrated a successful public key infrastructure (PKI) certificate exchange using United Kingdom and Slovenia systems in a multi-country test environment. Showcasing a "point-and-click" PKI system, Entrust confirmed that the security infrastructure for second-generation ePassports, based on Extended Access Control (EAC), is truly ready for global deployment.

"We didn't go to the Prague tests to get the PKI certificate exchange mostly right. We went with the goal of achieving a perfect score; and that's what we did," said Entrust Chairman, President and CEO Bill Conner. "As only two of four countries that signed up for all four PKI tests, we were extremely proud of our customers -- Slovenia and UK -- for stepping up to the plate and helping us demonstrate a flawless execution of our EAC PKI offering. That they had the level of confidence in our PKI to execute the tests for the world to see is a testament to our team and EAC."

Taking place over five days, one of the key objectives of the Prague tests was for European countries to prove the standards conformance of their ePassports containing fingerprint biometric data protected by EAC functions. A second objective was to verify crossover interoperability between EAC inspection systems and ePassports from different countries.

"We are pleased to have been able to team with Entrust to provide 'end-to-end' second-generation ePassport capability for Slovenia," said Bob LaPenta, founder and chief executive officer of L-1 Identity Solutions. "This is a critical step in the evolution and testing of government credentials utilizing more secure biometric and certificate capabilities. Our integration and interoperability results speak for themselves."

In addition to standard conformance and crossover interoperability, the tests were the first organized attempt to verify EAC PKI operation in accordance with the European Union Certificate Policy, including bilateral exchange of EAC certificates. Twelve of the 27 participating countries completed the first PKI test round, and four countries participated in all four phases of the PKI testing, demonstrating a complete end-to-end system.

While all twelve countries demonstrated certificate exchanges with multiple country certificate authorities, United Kingdom and Slovenia completed the four PKI test phases, as well as targeted exchanges with all 12 countries. As part of the event, Entrust also demonstrated integration with leading ePassport equipment vendors, including L-1, 3M and G.E.T.

"Participating in the Prague event helped us demonstrate our leadership by moving to second-generation ePassports," said Bojan Trnovsek, general director of the Internal Affairs Directorate at the Slovenian Ministry of Interior. "Entrust is a leader in the public key infrastructure (PKI) technology that helps strengthen and secure the foundation of our ePassport environment, and we're eager to realize the capabilities of this second-generation ePassport standard."

Facilitated by a consortium of the European Commission, Brussels Interoperability Group (BIG) and the European Commission Joint Research Centre, the Prague tests allowed European countries to verify conformance of their second-generation ePassports containing fingerprint biometric data protected by Extended Access Control functions, commonly referred to as EAC. Additional testing included verification of crossover interoperability between EAC inspection systems and ePassports from different countries.

"The rigorous testing in Prague was a critical step in the European deployment of second-generation ePassports," said Chairman of the Brussels Interoperability Group, Bob Carter, who also represents the United Kingdom Identity and Passport Service. "All countries that participated in this first test of the Extended Access Control PKI infrastructure successfully completed the tests, and with that success, the vision for an EAC-enabled ePassport deployment is becoming a reality. Entrust's PKI operated flawlessly last week, and it will serve as a strong security foundation for our deployment of EAC-enabled ePassports."

Countries are beginning to evolve their ePassport programs to the second generation, which includes enhanced security and privacy capabilities. European Union (EU) member countries are required to add advanced biometric data to their machine-readable travel documents (MRTDs) by June 2009.

"Getting any security implementation right takes the concerted effort from many dedicated experts, and that was amply demonstrated by the unprecedented cross-jurisdiction trust management at the heart of the EAC standard," said Conner. "Stringing together a few open-source components without extremely careful consideration can result in a dangerous implementation. We are in our eighth generation of our core PKI offering. As a result, our EAC PKI product has evolved to point-and-click usability and is ready for prime time."

The terrorists of 9/11 modified paper passports to cross borders while traveling into the United States. This highlighted the need for a more secure passport. In moving to electronic passports, the International Civil Aviation Organization (ICAO) touted two primary goals: to ensure a forged or modified passport could not be used to cross borders and to prevent a criminal from impersonating the holder of a genuine passport.

Created to mitigate passport forgery, first-generation ePassports place a simple biometric (typically a facial photo) along with a duplicate of the identity information contained in the paper document on an RFID chip and protect it using Basic Access Control (BAC). Entrust provides the digital signatures on BAC ePassports that prevent a modified passport from being used to successfully cross a border if properly processed.

The second-generation of ePassports, based on Extended Access Control, allows governments to leverage a stronger biometric (typically a fingerprint or iris scan) that is more difficult to impersonate. They require the passport reader to authenticate itself to the chip, thereby preventing 'skimming', the practice of an unauthorized reader interrogating the chip and extracting sensitive personal information. EAC ePassports also strengthen the encryption of the communication between the chip and the reader; thereby preventing eavesdropping of the biometric data.

Because of the requirement for the chip to authenticate the reader, the PKI requirements are much higher, demanding a vendor that can provide scalability, reliability and unprecedented performance. It is this PKI foundation that allows ePassports to be read at border stations, but not by criminals who may seek access to the data for purposes of manipulation or impersonation.

Entrust has a long history of providing security software and services to government agencies across the world. Entrust provides security solutions for e-government and national security initiatives in more than 30 countries worldwide. Government agencies are leveraging the flexible and scalable solutions that Entrust offers to secure transactions and information internally and with citizens, businesses, suppliers and contractors.

The top e-governments in the world rely on Entrust. As ranked by Accenture, the top seven e-governments in the world, including Singapore, Canada, the United Kingdom, the United States, Denmark, Sweden and Norway, use Entrust solutions to protect sensitive information and enable secure online services.

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in more than 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit <http://www.entrust.com/>.

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All Entrust product names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners.

For more information:

Lindsey Jones
Media Relations
972-728-0374
lindsey.jones@entrust.com