CERIAS

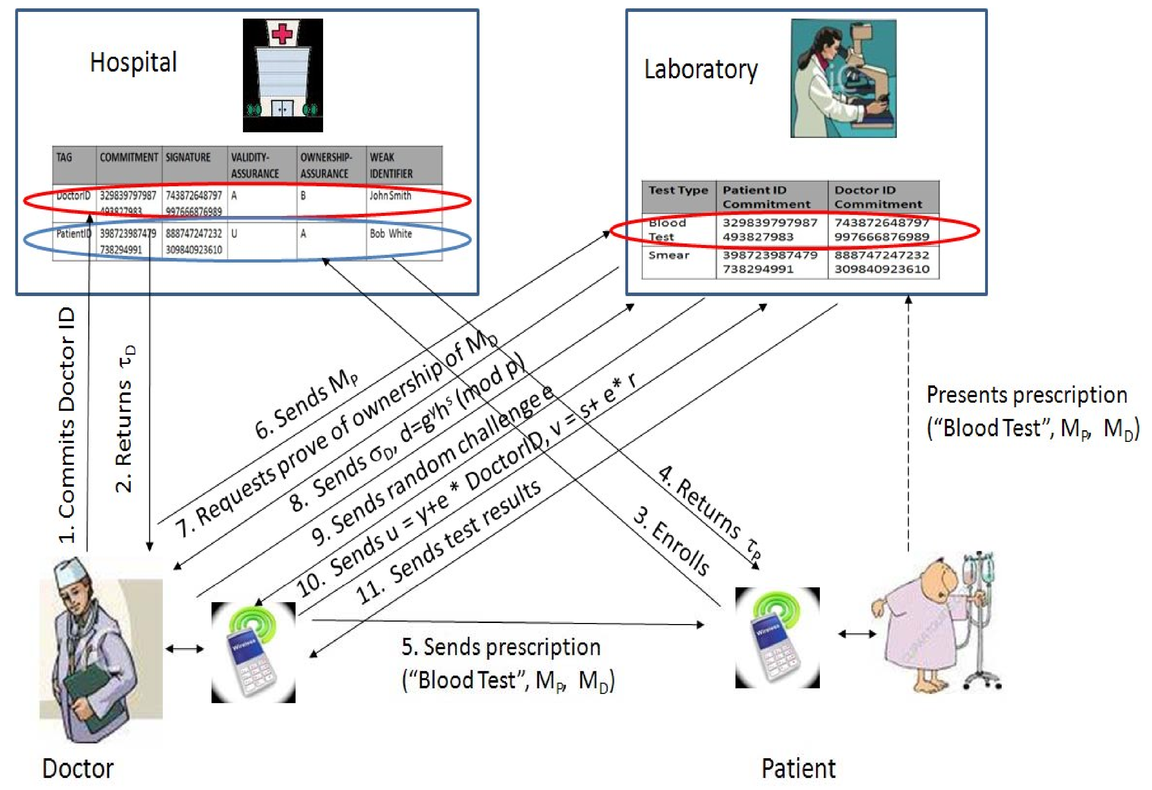
the center for education and research in information assurance and security

VeryIDX- A Privacy Preserving Digital Identity Management System for Mobile Devices

Federica Paci, Ning Shang , Kevin Steuer Jr, Sam Kerr, Ruchith Fernando
CS Department, Purdue University

- VeryIDX is a privacy-preserving digital identity management system based on the concept of multi-factor identity verification.

- Privacy is preserved by using secure cryptographic commitments and zero knowledge proof of knowledge protocols.



Application Scenario

1. ***Doctor Enrollment.*** Dr. Smith connects to the hospital portal and establishes an identity record IdR_D.
2. ***Patient Enrollment****.* A patient BoB by using its mobile device, connects to the hospital portal and establishes an identity record IdR_P.
3. ***Doctor prescribes a test to the Patient****.* Dr. Smith sends Bob an e-prescription that contains , the commitment of Bob patient identifier, M_P, and the commitment of Dr. Smith's doctor identifier, M_D.
4. ***Doctor Authentication at the Lab.*** Dr. Smith sends to the lab M_P and M_D. Based on M_P,, the lab retrieves the blood test results and asks Dr.Smith to prove ownership of M_D, that is included in the e-prescription provided by Bob to the lab.