MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Signatures ⇒ Entity authentication). *Construct an identification scheme that is based on a signature scheme. Prove that the corresponding identification scheme is secure in the most powerful setting, where the adversary can run several identification protocols concurrently in order to impersonate true signer.*

Solution.