Attestation Protocols: A Tutortial Introduction

Perry Alexander Brigid Halling

October 7, 2012

Contents

List of Figures

List of Tables

Abstract

This document is intended to provide a tutorial overview of the basic attestation protocols used by a TPM.

1 Introduction

2 Privacy Certificate Authority Based Attestation

There are two versions of the Privacy CA attestation process, one documented by Ryan [2009] and the other documented in the TCG specification [—, 2007]. They are not dramatically different, but should be reconciled.

2.1 The Ryan Approach

The Ryan protocol, shown in figure 1, is documented in his invaluable technical report Ryan [2009]. We have enhanced it here to include more explicit interaction between the appraiser and the user software.

1. An appraiser sends an attestation request indicating what PCRs are needed using a PCR make along with a nonce, n. (This request is not formally documented, but its specifics are not critical for this discussion.)
2. The user software receives the request and requests a fresh AIK from the TPM, wrapped with the TPM's SRK using the `TPM_MakeIdentity` command. Parameters to the `TPM_MakeIdentity` command describe properties of the desired AIK pair.
3. The TPM responds to the `TPM_MakeIdentity` command by generating a new AIK wrapped by SRK, installing the new AIK, and returning AIK, signed by the TPM using AIK^{-1} – $\{|AIK|\}_{AIK^{-1}}$.
   WHAT IS CR??? IS CR THE SIGNED KEYS?
   The new AIK is a key wrapped by SRK. The only way that $\{|AIK|\}_{AIK^{-1}}$ *can be created is in the presence of the TPM that generated AIK.*
4. The user software sends the certified public EK ($\{|EK|\}_{AIK^{-1}}$) and the signed public AIK ($\{|AIK|\}_{AIK^{-1}}$) obtained from the TPM to the Privacy CA and requests that it certify AIK.
5. The Privacy CA uses AIK to check the signature on EK and then determines if it has been revoked. It then uses AIK to check the signature on itself. If AIK signature check and EK signature check succeed, the Privacy CA knows the AIK and EK came from the same TPM. If both checks are successful, the Privacy CA signs the public AIK and encrypts the certificate with a fresh session key. It they encrypts both the new session key and the AIK with EK and returns both to the user software.
6. The user software uses the `TPM_ActivateIdentity` command to decyrpt the session key ($\{K\}_{EK}$). Only the TPM associated with EK can decrypt the session key. The user software then turn decrypts the signed AIK ($\{\{|AIK|\}_{CA^{-1}}\}_K$) using K. The (AIK) signed by the Privacy CA ($\{|AIK|\}_{CA^{-1}}$) can only be obtained in the presence of the TPM associated with EK. *This is exactly the result that we want.*
7. The user software requests a quote from the TPM using the `TPM_Quote` command and the nonce, n, sent by the appraiser. The TPM produces the quote, signed using AIK^{-1}. $\{|AIK|\}_{CA^{-1}}$ is also signed with AIK^{-1}. The user software sends the signed, certified AIK and signed quote back to the appraiser.
8. The appraiser analyzes the signed blobs received from the user software as follows:
   (a) AIK is used to check the signature of $\{|\{|AIKCA|\}_{|^{-1}}\}_{AIK^{-1}}$ — The certified AIK was signed by the same TPM as the quote.
   (b) CA is used to check the signature of $\{|AIK|\}_{CA^{-1}}$ — The Privacy CA has certified the AIK as coming from a legitimate TPM.
   (c) AIK is used to check the quote signature — The quote sent was signed by the TPM associated with the AIK.
   (d) n is checked against the nonce sent with the original request — The TPM quote is fresh.
   (e) PCRs from the quote are compared with expected values — The remote system is configured as expected.

2.2 TCG Documentation Approach

The TCG protocol, shown in figure 2, is documented in the TPM technical documentation by way of describing the TPM command set provided [—, 2007]. At this time, the distinction is the `TPM_MakeIdentity` command returning a signed public EK in addition to the signed AIK. If we can determine that this is the same as the certification request (CR), then the two protocols are basically the same.

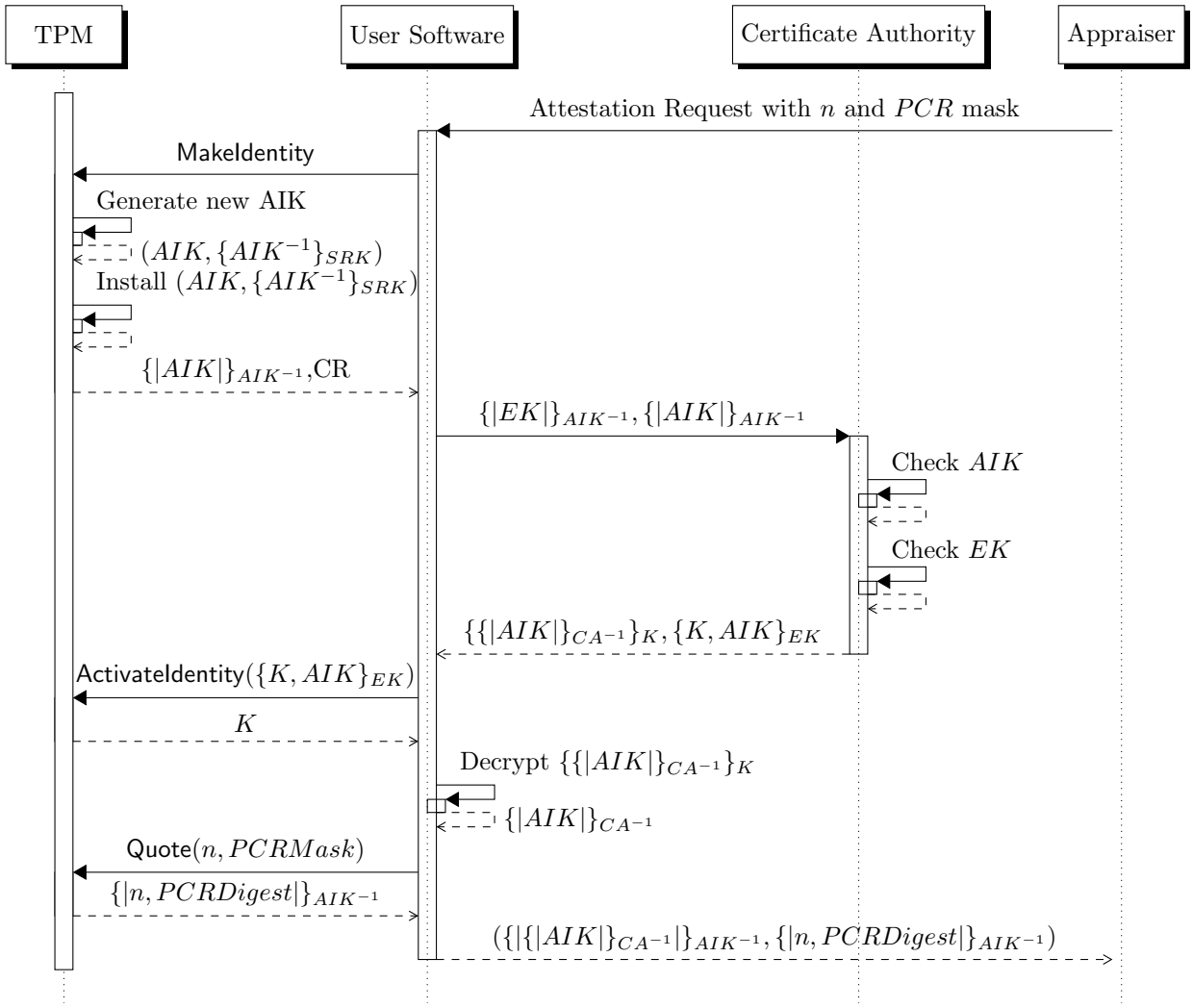

Figure 1: Sequence Diagram for the Privacy CA protocol as described by Ryan

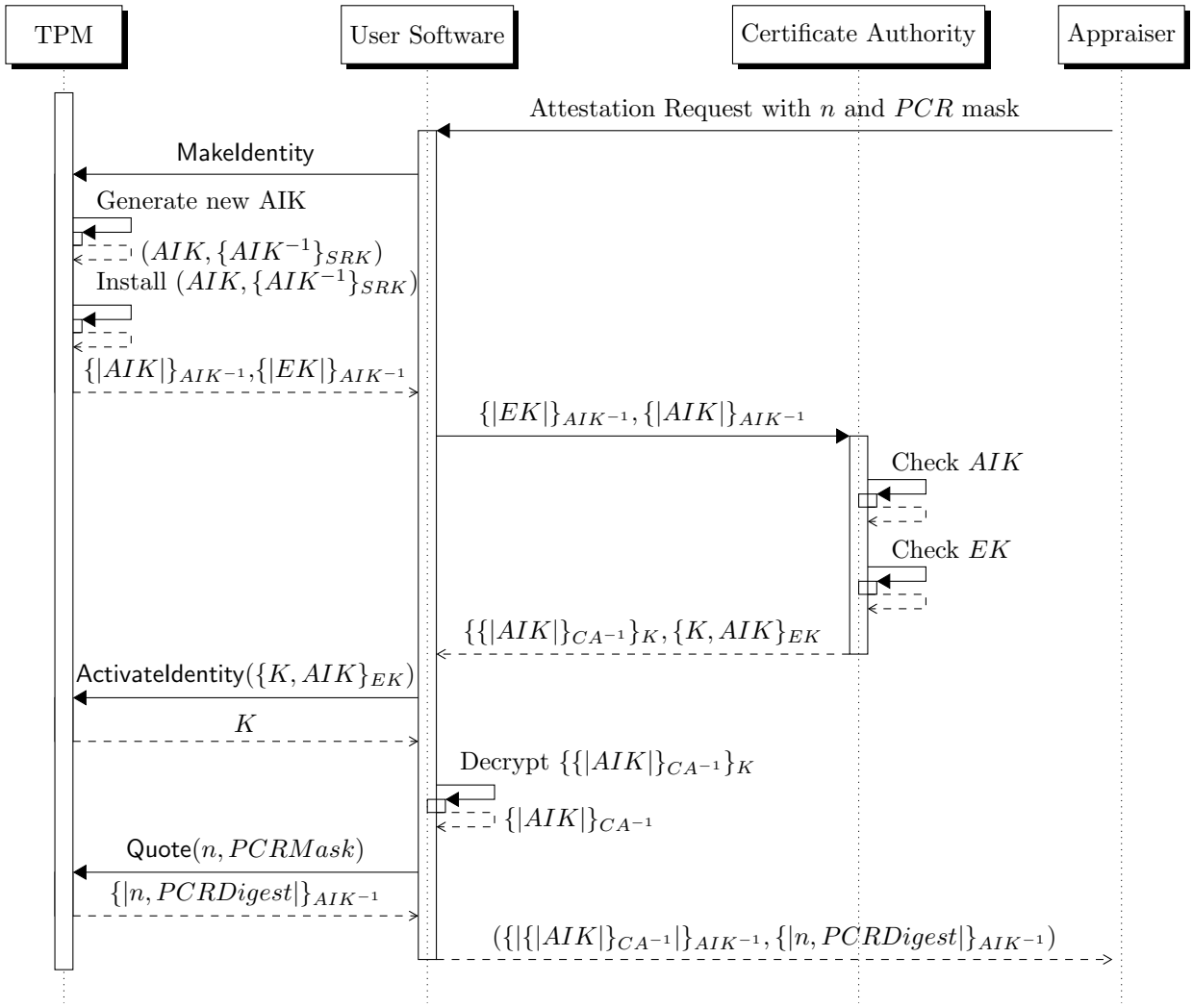

Figure 2: Sequence Diagram for the Privacy CA protocol as described by Ryan

3 Direct Anonymous Attestation

4 Glossary

$\{|M|\}_{K^{-1}}$ — M signed with private K.

$\{M\}_K$ — M encrypted with public K.

References

—. *TCG TPM Specification*. Trusted Computing Group, 3885 SW 153rd Drive, Beaverton, OR 97006, version 1.2 revision 103 edition, July 2007. URL `https://www.trustedcomputinggroup.org/resources/tpm_main_specification/`.

M. Ryan. Introduction to the tpm 1.2. Draft Report, March 2009.