

Title (en)  
METHOD FOR READING AN ATTRIBUTE FROM AN ID TOKEN

Title (de)  
VERFAHREN ZUM LESEN EINES ATTRIBUTS AUS EINEM ID-TOKEN

Title (fr)  
PROCÉDÉ DE LECTURE D'UN ATTRIBUT À PARTIR D'UN JETON ID

Publication  
**EP 2561461 A1 20130227 (DE)**

Application  
**EP 11717537 A 20110420**

Priority

- DE 102010028133 A 20100422
- EP 2011056315 W 20110420

Abstract (en)  
[origin: WO2011131715A1] The invention relates to a method for reading at least one attribute stored in an ID token (106, 106') using first (136), second (150) and third (100) computer systems, wherein the third computer system comprises a browser (112) and a client (113), and wherein a service certificate (144) is assigned to the second computer system, wherein the service certificate comprises an identifier which is used to identify the second computer system, wherein the ID token is assigned to a user (102), having the following steps: - a first cryptographically protected connection (TLS1) is set up between the browser of the third computer system and the second computer system, wherein the third computer system receives a first certificate (176), - the first certificate is stored by the third computer system, - the third computer system receives a signed attribute specification (182) via the first connection, - a second cryptographically protected connection (TLS2) is set up between the browser of the third computer system and the first computer system, wherein the third computer system receives a second certificate (190), - the signed attribute specification is forwarded from the third computer system to the first computer system via the second connection, - the first computer system accesses an authorization certificate (186), wherein the authorization certificate comprises the identifier, - a third cryptographically protected connection (TLS3) is set up between the first computer system and the client of the third computer system, wherein the third computer system receives the authorization certificate containing the identifier via the third connection, - the client of the third computer system checks whether the first certificate comprises the identifier as proof of the fact that the first certificate matches the service certificate, - the user is authenticated with respect to the ID token, - the first computer system (136) is authenticated with respect to the ID token, - a fourth cryptographically protected connection with end-to-end encryption is set up between the ID token and the first computer system, - after the user and the first computer system have been successfully authenticated with respect to the ID token, the first computer system has read access to the at least one attribute stored in the ID token via the fourth connection in order to read the one or more attributes specified in the attribute specification from the ID token, - the first computer system transmits the at least one attribute to the second computer system (150) after said attribute has been signed.

IPC 8 full level  
**G06F 21/00** (2013.01); **G06F 21/33** (2013.01); **G06F 21/34** (2013.01); **G06F 21/41** (2013.01)

CPC (source: EP US)  
**G06F 21/33** (2013.01 - EP US); **G06F 21/34** (2013.01 - EP US); **G06F 21/41** (2013.01 - EP US); **H04L 63/0428** (2013.01 - US); **H04L 63/0823** (2013.01 - EP US); **H04L 63/102** (2013.01 - EP US); **H04L 63/1466** (2013.01 - EP US)

Citation (examination)  
"Technische Richtlinie eID-Server", TECHNISCHE RICHTLINIE EID-SE, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, DE, no. BSI TR-03130 Version: 1.0 RC1, 19 May 2009 (2009-05-19), pages 1 - 48, XP007915025

Designated contracting state (EPC)  
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)  
**DE 102010028133 A1 20111027**; CN 102834830 A 20121219; CN 102834830 B 20160817; EP 2561461 A1 20130227; EP 4357945 A2 20240424; EP 4357945 A3 20240724; US 2013219181 A1 20130822; US 2015026476 A1 20150122; US 8812851 B2 20140819; US 9130931 B2 20150908; WO 2011131715 A1 20111027

DOCDB simple family (application)  
**DE 102010028133 A 20100422**; CN 201180018310 A 20110420; EP 11717537 A 20110420; EP 2011056315 W 20110420; EP 23208338 A 20110420; US 201113637691 A 20110420; US 201414452633 A 20140806