InterDigital®

novalyst IT®
knowledge & technology transfer

09/21/2010

Smart OpenID

Smart mobility

SMARTEVENT '10

Smart OpenID
Smartcard Webserver Enabled SSO for Web 2.0 using OpenID

Andreas Leicher, Andreas U. Schmidt (Novalyst IT),

Inhyok Cha, Yogendra Shah (InterDigital Communications)

With valuable contributions from:
Mike Meyerstein (Meyerstein Consulting LLC),
Louis Guccione (InterDigital Communications)

Smart mobility

SMARTEVENT '10

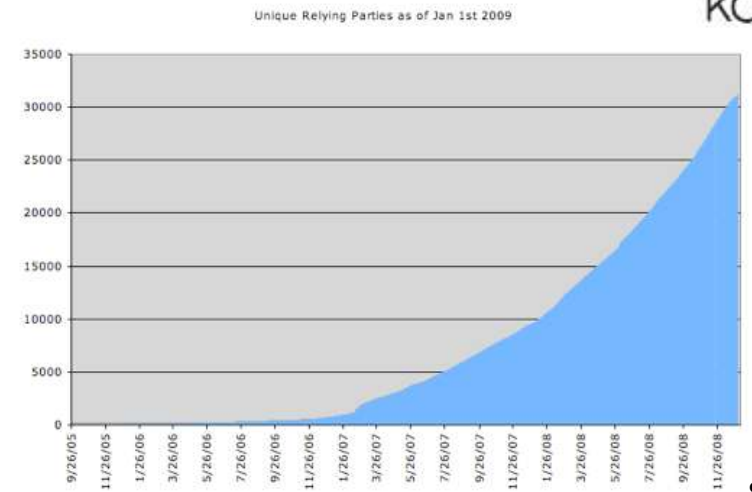
OpenID Technology

- OpenID is a lightweight, HTTP-based SSO protocol designed for Web2.0 applications
- OpenID provides a seamless user experience, one persistent online identity (represented by an URL) to be used across multiple Web services (relying parties, RP)
- Actual user authentication is not specified by OpenID, allowing for a broad range of different authentication schemes (pwd, card, token, biometrics, …)

- Relevance of OpenID for mobile markets and players is growing:
  - OpenID/GBA is being standardized in 3GPP SA3, TR 33.924
  - 3G Americas study on IdM for fixed and mobile networks
  - Major industry players such as Google have adopted OpenID

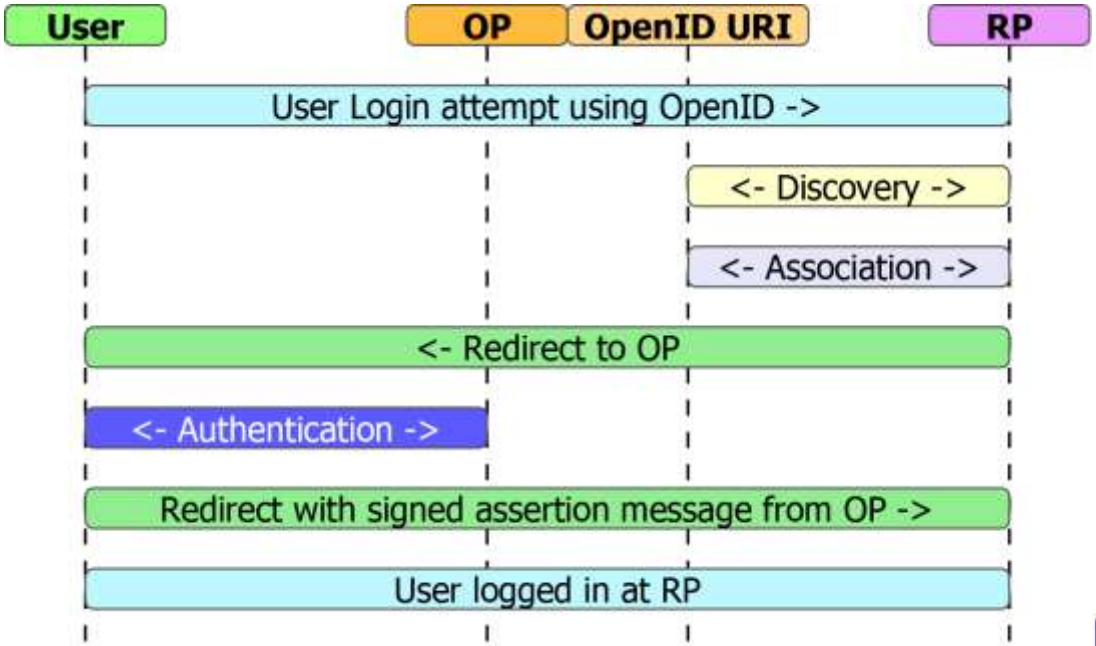
OpenID Industry Adoption and Support

- OpenID is an open, community based protocol and has large support from major industry players
- Growth of RPs accepting OpenID show an increasing trend
- OpenID started the OpenGovernment initiative to enable OpenID login on US federal websites
- Open Identity Exchange formed 2010; non-profit organization for building trust in the exchange of online identity credentials across public and private sectors (Google, PayPal, Equifax, VeriSign, Verizon, CA, and Booz Allen Hamilton)
- Kantara Initiative: Assurance and interoperability of IdM technologies: OpenID, Liberty AP, Infocard, …

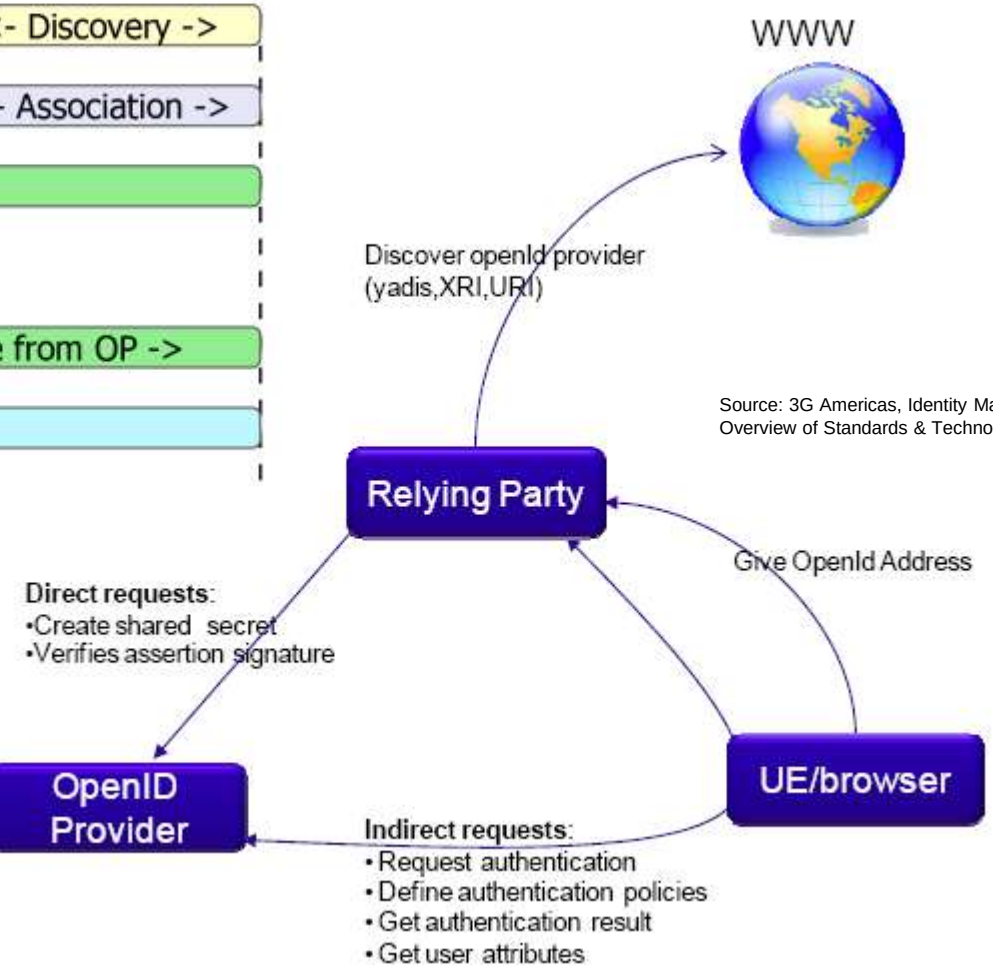


Source: janrain.com

OpenID Protocol



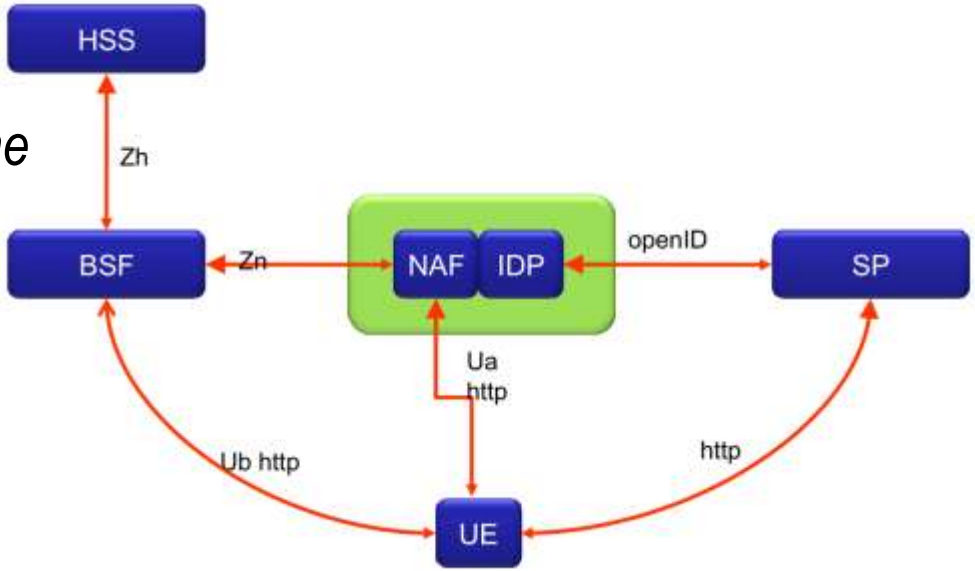
Source: own graphic, derived from OpenID Authentication 2.0 spec



Source: 3G Americas, Identity Mangement Overview of Standards & Technology

Standardization: OpenID/GBA

- Discussed in 3GPP SA3 in TR 33.924
- GBA is used to authenticate the user / UE via UICC
- Smart Card (UICC) is only used as authentication token
- The MNO acts as Identity Provider
- One GBA run is performed for every authentication
  - Every time any user logs in to any RP
- Problems
  - Can result in *heavy unpredictable load on the network* infrastructure for GBA authentication
  - Solution does *not take advantage of advanced smartcard features*



Source: 3G Americas, Identity Management Overview of Standards & Technology

Smart OpenID

OpenID OP Server on SCWS

RP website

User visits OpenID enabled site and requests OpenID login

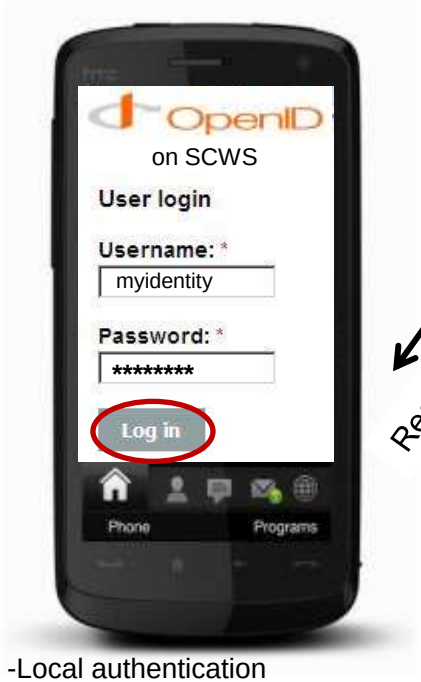
mymobile.myoperator/myidentity

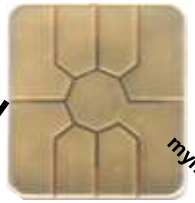
- The User logs in to the RP using OpenID and provides his OpenID identifier to the RP

Smart OpenID

OpenID OP Server
on SCWS

RP website





Request authentication

mymobile.myoperator/myidentity

-Local authentication
(towards OP on SCWS)
-Browser based
-Seamless integration
- local authentication
-No additional traffic

- The RP discovers OP and associates,
- The OP requests user authentication,
- The User enters his login credentials

Smart OpenID

RP website

OpenID OP Server
on SCWS

•verify password
•sign assertion message

assertion message

-Local authentication (towards OP on SCWS)
-Browser based
-Seamless integration

- The OP verifies the password and signs the assertion message, which is then sent to the RP
- The RP verifies the assertion message and the user is logged in

InterDigital®

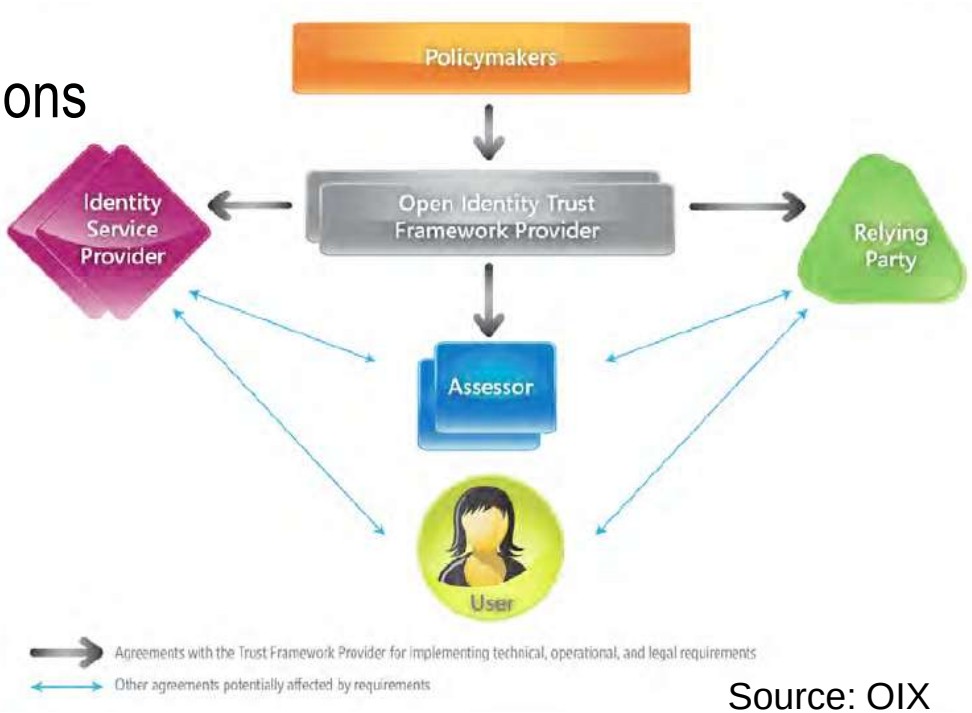
novalyst IT®

Benefits for Operators and Smart Card Manufacturers

- Value proposition from an Operator's Perspective
  - Operator anchored trust foundation for RPs (any Web service)
  - Branding: custom Operator web screen via SmartCard Web Server (SCWS)
  - Transparent identification and seamless authentication
- Viability from an Operator's perspective
  - Authentication can build upon existing and proven security of the smartcard
  - No additional network traffic for authentication beyond HTTP web access
  - No need to tailor application for different phone form factors
    - Leverages common platform for SmartCard Web Server on UICC
    - UICC is a controlled and manageable platform which avoids fragmented market for software/firmware developers in handsets
  - Mechanism for roll-out of Single-Sign-On solution is already in place for remote download via SMS

Details

- Instead of redirecting the user to the OP, the user is redirected to the SCWS inside his device
- OP application logic is implemented in the smartcard
- The user shares his authentication credentials over a local user interface with the local OP
- RPs do not have to change existing OpenID implementations
- RPs can leverage increased level of trust in smartcard based authentication
- MNO and smartcard issuer act as Trust Framework Provider

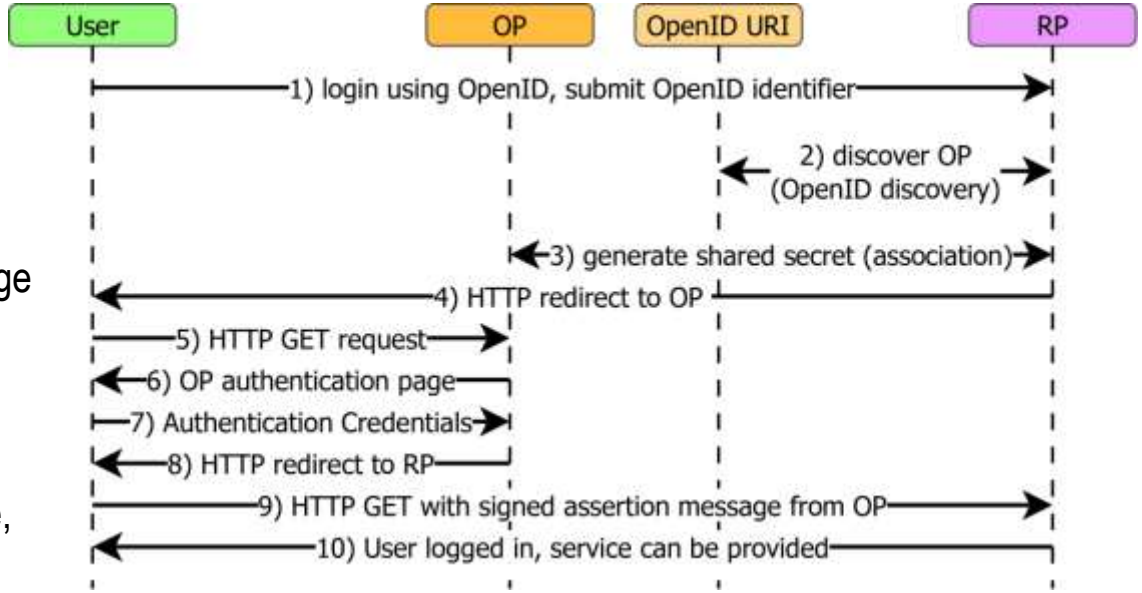


Source: OIX

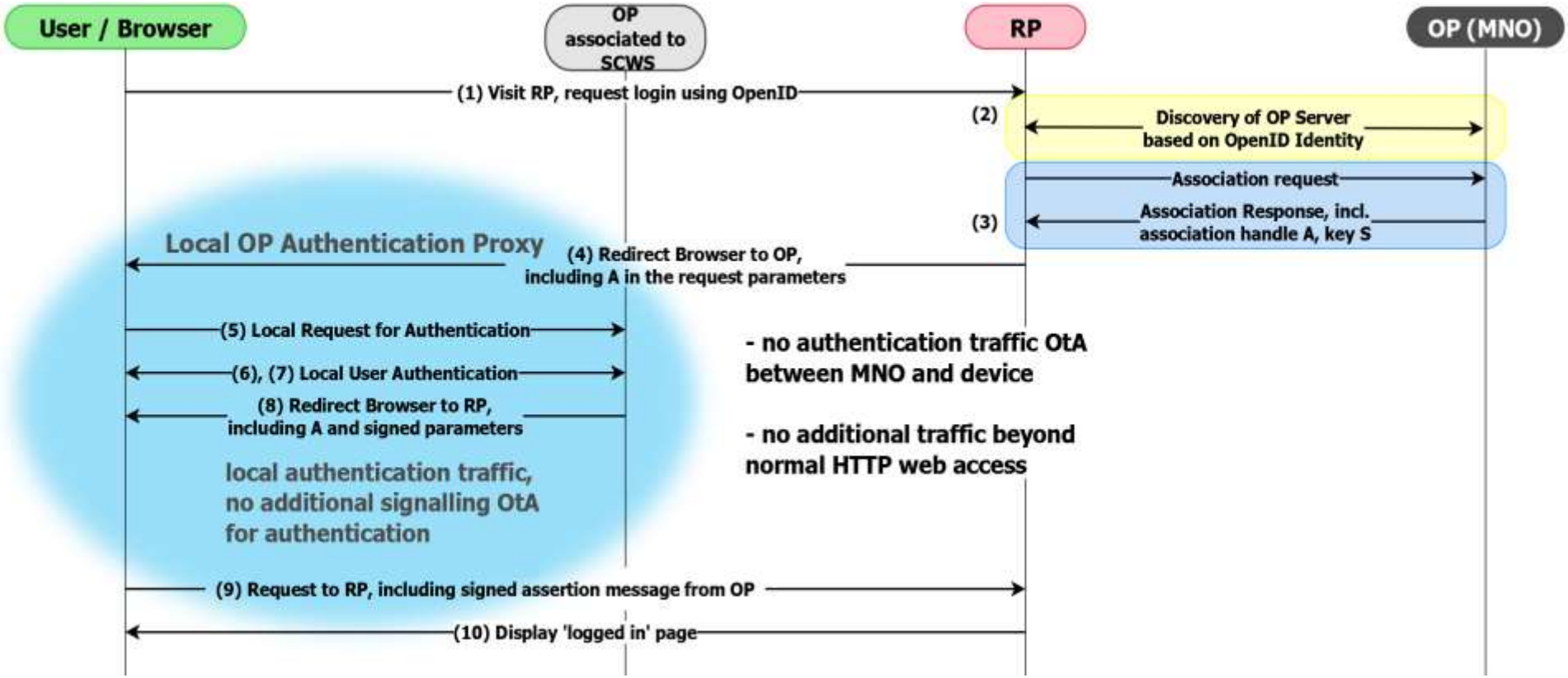
Standard OpenID Protocol Flow

- 3 parties: **Identity Provider** (OP), **Relying Party** (RP) and **User**

1. User uses identifier (URL) to log in to RP
2. RP discovers OP from given URL
3. RP establishes a shared secret with the OP
4. RP redirects the user to his OP
5. The user sees the authentication page of his OP
6. OP requests user credentials
7. User authenticates towards his OP
8. The OP signs an assertion message, and redirects the user to RP
9. User is redirected to RP and the RP can verify the signed assertion
10. User is logged in



Simple Smart OpenID Protocol Flow



Development Stage and Way Forward

- Feasibility study according to OMA, GP and ETSI SCP standards:
  - ETSI TS 102 412: Smart Card Platform requirements, v9.0.1
  - OMA "Smartcard-Web-Server", OMA “Smartcard-Web-Server-Requirements”
  - Global Platform Card Specification v2.2
  - TS 33.220 Generic Bootstrapping Architecture
  - ETSI TS 102 221: UICC-Terminal interface
  - TS 102 484 Smart Cards; Secure Channel between a UICC and an end-point Terminal
- Protocol flow demonstration challenges:
  - Work around restrictions of SCWS
  - Design of protocol flow must remain compatible to standard OpenID to benefit from large base of RPs
- Future and next steps:
  - **Prototype on Smart Card**
  - **Test deployment**

Smart mobility

SMARTEVENT '10

THANK YOU

Contact

novalyst IT®
knowledge & technology transfer

Dr. Andreas U. Schmidt
andreas.schmidt@novalyst.de

Andreas Leicher
andreas.leicher@novalyst.de

Novalyst IT AG
Robert-Bosch-Str. 38
61184 Karben, Germany

InterDigital®

Dr. Yogendra Shah
yogendra.shah@interdigital.com

Dr. Inhyok Cha
inhyok.cha@interdigital.com

InterDigital Communications, LLC
781 Third Avenue, King of Prussia, PA 19406, USA

InterDigital® novalyst IT®