INTEGRITY SECURITY SERVICES
A Green Hills Software Company

INTEGRITY Security Services, Inc.
V2X Root Certificate Authority (CA)

Certificate Profile

Version 1.0

March 31, 2016

INTEGRITY Security Services, Inc.
a Green Hills Software Company

INTEGRITY SECURITY SERVICES
A Green Hills Software Company

V2X Root CA Certificate Profile

```
RootCaCertificate ::= ExplicitCertificate (WITH COMPONENTS { ...,
  issuer (WITH COMPONENTS {self}),
  toBeSigned (WITH COMPONENTS { ...,
    id (WITH COMPONENTS {
      name ("v2xrootca.ghsiss.com")
    }),
    cracaId('000000'H),
    crlSeries(0),
    validityPeriod (WITH COMPONENTS { ...,
      duration (RootCaCertExpiration)
    }),
    region ABSENT,
    assuranceLevel ABSENT,
    appPermissions (SequenceOfPsidSsp (SIZE(2)) (CONSTRAINED BY {
      PsidSsp (WITH COMPONENTS {
        psid (SecurityMgmtPsid),
        ssp --OER encoding of ScmsSsp indicating RootCaSsp
      }),
      PsidSsp (WITH COMPONENTS {
        psid (CrlPsid),
        ssp (WITH COMPONENTS {opaque(CONTAINING CrlSsp (WITH
COMPONENTS {...,
          associatedCraca(isCraca),
          crls (PermissibleCrls (SIZE(1)) (CONSTRAINED BY {
            CrlSeries (ScmsSpclComponentCrlSeries)
          }))
        }))}})
      })
    })),
    certIssuePermissions (SequenceOfPsidGroupPermissions (SIZE(4))
(CONSTRAINED BY {
      PsidGroupPermissions ( WITH COMPONENTS {...,
        subjectPermissions (WITH COMPONENTS {
          all
        }),
        minChainDepth(3),
        chainDepthRange(-1),
        eeType ({app, enrol})
      }),
      PsidGroupPermissions ( WITH COMPONENTS {...,
        subjectPermissions (WITH COMPONENTS{
```

```
          explicit (SequenceOfPsidSspRange (SIZE (1)) (WITH COMPONENT
(WITH COMPONENTS {
            psid (SecurityMgmtPsid), sspRange ABSENT
          }))
        }),
        minChainDepth(1),
        chainDepthRange(-1),
        eeType ({app, enrol})
      }),
      PsidGroupPermissions ( WITH COMPONENTS {...,
        subjectPermissions (WITH COMPONENTS{
          explicit (SequenceOfPsidSspRange (SIZE (1)) (WITH COMPONENT
(WITH COMPONENTS {
            psid (MisbehaviorReportingPsid), sspRange ABSENT
          }))
        }),
        minChainDepth(1),
        chainDepthRange(-1),
        eeType ({app, enrol})
      }),
      PsidGroupPermissions ( WITH COMPONENTS {...,
        subjectPermissions (WITH COMPONENTS{
          explicit (SequenceOfPsidSspRange (SIZE (1)) (WITH COMPONENT
(WITH COMPONENTS {
            psid (CrlPsid), sspRange (WITH COMPONENTS {all})
          }))
        }),
        minChainDepth(1),
        chainDepthRange(-1),
        eeType ({app, enrol})
      })
    })),
    certRequestPermissions ABSENT,
    canRequestRollover ABSENT,
    encryptionKey ABSENT,
    verifyKeyIndicator (WITH COMPONENTS {
      verificationKey (WITH COMPONENTS {
        ecdsaNistP256 (WITH COMPONENTS {
          compressed-y-0, compressed-y-1
        })
      })
    })
  })
})
```

Notes:

For this profile, the following terms are defined as follows:

```
      Validity Period Start      385689600
```

RootCaCertExpiration	70 years
ScmsSpclComponentCrlSeries	256
SecurityMgmtPsid	35
MisbehaviorReportingPsid	38
CrlPsid	256

JSON Notation of Root CA Certificate

The following is the JSON representation of the actual V2X Root CA's certificate. Note the public key and signature fields are "x'd" out for legibility.


```
{
    "version": 3,
    "type": "explicit",
    "issuer": {
        "self": "sha256"
    },
    "toBeSigned": {
        "id": {
            "name": "v2xrootca.ghsiss.com"
        },
        "cracaId": "000000",
        "crlSeries": 0,
        "validityPeriod": {
          "start": 385689600,
          "duration": {
                "years": 70
          }
        },
        "appPermissions": [
            {
                "psid": 35,
                "ssp": {
                    "opaque": "810001"
                }
            },
            {
                "psid": 256,
                "ssp": {
                    "opaque": "00010001010100"
                }
            }
        ],
        "certIssuePermissions": [
            {
                "subjectPermissions": {
                    "all": null
                },
```

```
                "minChainDepth": 3,
                "chainDepthRange": -1,
                "eeType": "C0"
            },
            {
                "subjectPermissions": {
                    "explicit": [
                        {
                            "psid": 35
                        }
                    ]
                },
                "minChainDepth": 1,
                "chainDepthRange": -1,
                "eeType": "C0"
            },
            {
                "subjectPermissions": {
                    "explicit": [
                        {
                            "psid": 38
                        }
                    ]
                },
                "minChainDepth": 1,
                "chainDepthRange": -1,
                "eeType": "C0"
            },
            {
                "subjectPermissions": {
                    "explicit": [
                        {
                            "psid": 256,
                            "sspRange": {
                                "all": null
                            }
                        }
                    ]
                },
                "minChainDepth": 1,
                "chainDepthRange": -1,
                "eeType": "C0"
            }
        ],
        "verifyKeyIndicator": {
            "verificationKey": {
                "ecdsaNistP256": {
                    "compressed-y-0":
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
                }
            }
        }
```

```
    },
    "signature": {
        "ecdsaNistP256Signature": {
            "r": {
                "x-only":
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
            },
            "s":
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
        }
    }
}
```

Revision History

1.0 Released to CAMP 31 March 2016.